

日 本 国 特 許 庁
JAPAN PATENT OFFICE

JKY
Jc781 U.S. PTO
10/021331
12/12/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2000年12月13日

出 願 番 号

Application Number:

特願2000-378261

出 願 人

Applicant(s):

ソニー株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年11月16日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3099702

【書類名】 特許願

【整理番号】 0000776311

【提出日】 平成12年12月13日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 17/60
G09C 1/00
G06K 5/00

【発明者】

【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内

【氏名】 飯野 陽一郎

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代表者】 出井 伸之

【代理人】

【識別番号】 100082131

【弁理士】

【氏名又は名称】 稲本 義雄

【電話番号】 03-3369-6479

【手数料の表示】

【予納台帳番号】 032089

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9708842

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報記録媒体、情報処理装置および情報処理方法、プログラム記録媒体、並びに情報処理システム

【特許請求の範囲】

【請求項1】 それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データと、

前記秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、前記有効性データによって、その有効性が証明される被証明情報とが記録されている

ことを特徴とする情報記録媒体。

【請求項2】 前記有効性データと被証明情報とは、電子的なチケットである電子チケットを構成する

ことを特徴とする請求項1に記載の情報記録媒体。

【請求項3】 前記被証明情報は、前記電子チケットの権利内容を、さらに含む

ことを特徴とする請求項2に記載の情報記録媒体。

【請求項4】 前記被証明情報は、その改竄を行うことができないように処理されている

ことを特徴とする請求項3に記載の情報記録媒体。

【請求項5】 前記被証明情報には、電子署名が含まれることにより、その改竄を行うことができないように処理されている

ことを特徴とする請求項4に記載の情報記録媒体。

【請求項6】 前記有効性データは、前記電子チケットの使用回数をさらに含む

ことを特徴とする請求項3に記載の情報記録媒体。

【請求項7】 前記有効性データは、暗号化されている

ことを特徴とする請求項1に記載の情報記録媒体。

【請求項8】 前記有効性データは、所定の鍵で暗号化され、

前記所定の鍵は、別の鍵で暗号化されている

ことを特徴とする請求項 7 に記載の情報記録媒体。

【請求項 9】 前記秘密情報は、公開鍵暗号化方式の秘密鍵であり、

前記検証用パラメータは、前記秘密鍵に対応する公開鍵である

ことを特徴とする請求項 2 に記載の情報記録媒体。

【請求項 10】 前記被証明情報は、前記電子チケットの発行者を識別するための発行者識別情報、前記発行者を検証するための公開鍵、および前記発行者識別情報と公開鍵に対して、所定の認証センタが生成した電子署名からなる、前記発行者の証明書である発行者証明書をさらに含む

ことを特徴とする請求項 2 に記載の情報記録媒体。

【請求項 11】 それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データを生成する有効性データ生成手段と、

前記秘密情報が存在することを検証するのに用いられる検証用パラメータを生成する検証用パラメータ生成手段と、

前記検証用パラメータを含み、前記有効性データによって、その有効性が証明される被証明情報を生成する被証明情報生成手段と、

前記有効性データと被証明情報とからなる情報セットを外部に出力する出力手段と

を備えることを特徴とする情報処理装置。

【請求項 12】 前記有効性データと被証明情報とからなる情報セットは、電子的なチケットである電子チケットを構成する

ことを特徴とする請求項 11 に記載の情報処理装置。

【請求項 13】 前記被証明情報生成手段は、前記電子チケットの権利内容をさらに含む前記被証明情報を生成する

ことを特徴とする請求項 12 に記載の情報処理装置。

【請求項 14】 前記被証明情報生成手段は、前記被証明情報を、その改竄を行うことができないように処理する

ことを特徴とする請求項 13 に記載の情報処理装置。

【請求項 1 5】 前記被証明情報生成手段は、前記被証明情報に、電子署名を含めることにより、その改竄を行うことができないように処理する

ことを特徴とする請求項 1 4 に記載の情報処理装置。

【請求項 1 6】 前記出力手段は、前記電子チケットの情報としての前記有効性データおよび被証明情報を外部に出力する際に、出力相手の装置との間で認証処理を行う

ことを特徴とする請求項 1 2 に記載の情報処理装置。

【請求項 1 7】 前記出力手段は、前記有効性データを暗号化して出力することを特徴とする請求項 1 2 に記載の情報処理装置。

【請求項 1 8】 前記出力手段は、
公開鍵暗号化方式の公開鍵、およびその公開鍵に対して、所定の認証センタが生成した電子署名からなる、正当な装置であることを証明する装置証明書を、相手の装置に送信し、

前記相手の装置から送信されてくる暗号鍵であって、前記装置証明書に含まれる前記公開鍵で暗号化されたものを、前記公開鍵に対応する秘密鍵で復号し、

前記暗号鍵で、前記有効性データを暗号化する

ことを特徴とする請求項 1 7 に記載の情報処理装置。

【請求項 1 9】 前記有効性データ生成手段は、公開鍵暗号化方式の秘密鍵を、前記秘密情報としてを含む有効性データを生成し、

前記検証用パラメータ生成手段は、前記秘密鍵に対応する公開鍵を、前記検証用パラメータとして生成する

ことを特徴とする請求項 1 2 に記載の情報処理装置。

【請求項 2 0】 前記被証明情報生成手段は、前記電子チケットの発行者を識別するための発行者識別情報、前記発行者を検証するための公開鍵、および前記発行者識別情報と公開鍵に対して、所定の認証センタが生成した電子署名からなる、前記発行者の証明書である発行者証明書をさらに含む前記被証明情報を生成する

ことを特徴とする請求項 1 2 に記載の情報処理装置。

【請求項 2 1】 それ自体を外部に示すことなく、それが存在することを証

明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データを生成する有効性データ生成ステップと、

前記秘密情報が存在することを検証するのに用いられる検証用パラメータを生成する検証用パラメータ生成ステップと、

前記検証用パラメータを含み、前記有効性データによって、その有効性が証明される被証明情報を生成する被証明情報生成ステップと、

前記有効性データと被証明情報とからなる情報セットを外部に出力する出力ステップと

を備えることを特徴とする情報処理方法。

【請求項 2 2】 コンピュータに実行させるプログラムが記録されているプログラム記録媒体において、

それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データを生成する有効性データ生成ステップと、

前記秘密情報が存在することを検証するのに用いられる検証用パラメータを生成する検証用パラメータ生成ステップと、

前記検証用パラメータを含み、前記有効性データによって、その有効性が証明される被証明情報を生成する被証明情報生成ステップと、

前記有効性データと被証明情報とからなる情報セットを外部に出力する出力ステップと

を備えるプログラムが記録されている

ことを特徴とするプログラム記録媒体。

【請求項 2 3】 それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データと、

前記秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、前記有効性データによって、その有効性が証明される被証明情報と

からなる情報セットを処理する情報処理装置において、

前記情報セットを記憶する記憶手段と、

前記被証明情報を、その被証明情報を検査する検査装置に送信する被証明情報送信手段と、

前記秘密情報の存在を証明する証明データを生成し、前記検査装置に送信する証明データ生成手段と

を備えることを特徴とする情報処理装置。

【請求項 2 4】 前記有効性データと被証明情報とからなる情報セットは、電子的なチケットである電子チケットを構成する

ことを特徴とする請求項 2 3 に記載の情報処理装置。

【請求項 2 5】 前記有効性データを、第 1 の暗号鍵で暗号化する第 1 の暗号化手段と、

前記第 1 の暗号鍵で暗号化された前記有効性データを、前記第 1 の鍵で復号する第 1 の復号手段と

をさらに備え、

前記記憶手段は、前記第 1 の暗号鍵で暗号化された前記有効性データを記憶する

ことを特徴とする請求項 2 3 に記載の情報処理装置。

【請求項 2 6】 前記第 1 の暗号鍵は、所定のタイミングで更新されることを特徴とする請求項 2 5 に記載の情報処理装置。

【請求項 2 7】 前記第 1 の暗号鍵を、第 2 の暗号鍵で暗号化する第 2 の暗号化手段と、

前記第 2 の鍵で暗号化された前記第 1 の暗号鍵を、前記第 2 の暗号鍵で復号する第 2 の復号手段と

をさらに備え、

前記記憶手段は、前記第 2 の鍵で暗号化された前記第 1 の暗号鍵も記憶することを特徴とする請求項 2 5 に記載の情報処理装置。

【請求項 2 8】 前記第 2 の暗号鍵は、前記第 2 の暗号化手段および復号手段を構成するハードウェアに内蔵される

ことを特徴とする請求項 2 7 に記載の情報処理装置。

【請求項 2 9】 前記第 2 の暗号鍵は、所定のタイミングで更新される

ことを特徴とする請求項 2 7 に記載の情報処理装置。

【請求項 3 0】 前記被証明情報は、前記電子チケットの権利内容をさらに含む

ことを特徴とする請求項 2 4 に記載の情報処理装置。

【請求項 3 1】 前記被証明情報は、その改竄を行うことができないように処理されている

ことを特徴とする請求項 2 4 に記載の情報処理装置。

【請求項 3 2】 前記被証明情報は、電子署名が含まれることにより、その改竄を行うことができないように処理されている

ことを特徴とする請求項 3 1 に記載の情報処理装置。

【請求項 3 3】 前記秘密情報は、公開鍵暗号化方式の秘密鍵であり、
前記検証用パラメータは、前記秘密鍵に対応する公開鍵であり、
前記証明データ生成手段は、前記秘密鍵を用いた処理を行うことによって、前記証明データを生成する

ことを特徴とする請求項 2 4 に記載の情報処理装置。

【請求項 3 4】 前記有効性データは、前記電子チケットの使用回数を含み、
前記証明データ生成手段は、所定の情報と前記使用回数を、前記秘密鍵を用いて処理し、その処理結果と前記使用回数を送信する

ことを特徴とする請求項 3 3 に記載の情報処理装置。

【請求項 3 5】 前記証明データ生成手段により前記使用回数が送信されるごとに、前記記憶手段に記憶された前記有効性データに含まれる使用回数をインクリメントするインクリメント手段をさらに備える

ことを特徴とする請求項 3 4 に記載の情報処理装置。

【請求項 3 6】 前記記憶手段に記憶された前記有効性データおよび被証明情報からなる電子チケットの情報を、他の装置に譲渡する譲渡手段をさらに備える

ことを特徴とする請求項 2 4 に記載の情報処理装置。

【請求項 3 7】 前記電子チケットの情報を譲渡する際に、前記他の装置との間で認証処理を行う認証手段をさらに備える

ことを特徴とする請求項 3 6 に記載の情報処理装置。

【請求項 3 8】 前記譲渡手段は、前記有効性データを暗号化して、前記他の装置に送信する

ことを特徴とする請求項 3 6 に記載の情報処理装置。

【請求項 3 9】 前記譲渡手段は、

公開鍵暗号化方式の公開鍵、およびその公開鍵に対して、所定の認証センタが生成した電子署名からなる、正当な装置であることを証明する装置証明書を、前記他の装置に送信し、

前記相手の装置から送信されてくる暗号鍵であって、前記装置証明書に含まれる前記公開鍵で暗号化されたものを、前記公開鍵に対応する秘密鍵で復号し、

前記暗号鍵で、前記有効性データを暗号化する

ことを特徴とする請求項 3 8 に記載の情報処理装置。

【請求項 4 0】 前記譲渡手段は、前記電子チケットの情報を、他の装置に譲渡するとともに、その電子チケットの情報を、前記記憶手段から削除する

ことを特徴とする請求項 3 6 に記載の情報処理装置。

【請求項 4 1】 前記有効性データおよび被証明情報からなる電子チケットの情報を、他の装置から譲受する譲受手段をさらに備える

ことを特徴とする請求項 2 4 に記載の情報処理装置。

【請求項 4 2】 前記電子チケットの情報を譲受する際に、前記他の装置との間で認証処理を行う認証手段をさらに備える

ことを特徴とする請求項 4 1 に記載の情報処理装置。

【請求項 4 3】 前記譲受手段は、前記他の装置からの電子チケットの情報を構成する被証明情報の正当性を確認する

ことを特徴とする請求項 4 2 に記載の情報処理装置。

【請求項 4 4】 前記被証明情報は、前記電子チケットの発行者を識別するための発行者識別情報、前記発行者を検証するための公開鍵、および前記発行者識別情報と公開鍵に対して、所定の認証センタが生成した電子署名からなる、前記発行者の証明書である発行者証明書をさらに含み、

前記譲受手段は、前記発行者証明書に基づいて、前記被証明情報の正当性を確

認する

ことを特徴とする請求項43に記載の情報処理装置。

【請求項45】 前記被証明情報には、電子署名が含まれており、
前記譲受手段は、前記電子署名に基づいて、前記被証明情報の正当性を確認する

ことを特徴とする請求項43に記載の情報処理装置。

【請求項46】 前記被証明情報には、前記公開鍵に対応する秘密鍵によって生成された電子署名が付加されており、

前記譲受手段は、前記電子署名を、前記公開鍵で処理することにより、前記被証明情報の正当性を確認する

ことを特徴とする請求項44に記載の情報処理装置。

【請求項47】 前記譲受手段は、暗号化されている前記有効性データを受信する

ことを特徴とする請求項41に記載の情報処理装置。

【請求項48】 前記譲受手段は、

公開鍵暗号化方式の公開鍵、およびその公開鍵に対して、所定の認証センタが生成した電子署名からなる、正当な装置であることを証明する装置証明書を、前記他の装置から受信し、

所定の暗号鍵を、前記装置証明書に含まれる前記公開鍵で暗号化したものを、前記他の装置に送信し、

前記所定の暗号鍵で暗号化された前記有効性データを受信する

ことを特徴とする請求項47に記載の情報処理装置。

【請求項49】 それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データと、

前記秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、前記有効性データによって、その有効性が証明される被証明情報と

からなる情報セットを処理する情報処理方法において、

前記被証明情報を、その被証明情報を検査する検査装置に送信する被証明情報

送信ステップと、

前記秘密情報の存在を証明する証明データを生成し、前記検査装置に送信する証明データ生成ステップと

を備えることを特徴とする情報処理方法。

【請求項 5 0】 それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データと、

前記秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、前記有効性データによって、その有効性が証明される被証明情報と

からなる情報セットを、コンピュータに処理させるプログラムが記録されているプログラム記録媒体において、

前記被証明情報を、その被証明情報を検査する検査装置に送信する被証明情報送信ステップと、

前記秘密情報の存在を証明する証明データを生成し、前記検査装置に送信する証明データ生成ステップと

を備えるプログラムが記録されている

ことを特徴とするプログラム記録媒体。

【請求項 5 1】 それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データと、

前記秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、前記有効性データによって、その有効性が証明される被証明情報と

からなる情報セットを検査する情報処理装置において、

他の装置からの前記被証明情報を受信する被証明情報受信手段と、

前記他の装置からの前記秘密情報の存在を証明する証明データを受信する証明データ受信手段と、

前記証明データと、前記被証明情報に含まれる検証用パラメータとを用いて、前記他の装置における前記秘密情報の存否を判定する存否判定手段と

を備えることを特徴とする情報処理装置。

【請求項 5 2】 前記有効性データと被証明情報とからなる情報セットは、電子的なチケットである電子チケットを構成する

ことを特徴とする請求項 5 1 に記載の情報処理装置。

【請求項 5 3】 前記被証明情報は、前記電子チケットの権利内容を、さらに含み、

前記権利内容が、所定のサービス提供の条件を満たすかどうかを判定する権利内容判定手段をさらに備える

ことを特徴とする請求項 5 2 に記載の情報処理装置。

【請求項 5 4】 前記秘密情報は、公開鍵暗号化方式の秘密鍵であり、

前記検証用パラメータは、前記秘密鍵に対応する公開鍵であり、

前記証明データは、前記有効性データに含まれる前記秘密鍵を用いた処理を行うことにより生成されたものであり、

前記存否判定手段は、前記証明データを、前記公開鍵で処理することにより、前記秘密情報の存否を判定する

ことを特徴とする請求項 5 2 に記載の情報処理装置。

【請求項 5 5】 前記有効性データは、前記電子チケットの使用回数を含み、
前記証明データは、所定の情報と前記使用回数を、前記秘密鍵を用いて処理した処理結果と、前記使用回数とで構成される

ことを特徴とする請求項 5 4 に記載の情報処理装置。

【請求項 5 6】 前記他の装置からの電子チケットの情報を構成する被証明情報の正当性を確認する確認手段をさらに備える

ことを特徴とする請求項 5 2 に記載の情報処理装置。

【請求項 5 7】 前記被証明情報は、前記電子チケットの発行者を識別するための発行者識別情報、前記発行者を検証するための公開鍵、および前記発行者識別情報と公開鍵に対して、所定の認証センタが生成した電子署名からなる、前記発行者の証明書である発行者証明書をさらに含み、

前記確認手段は、前記発行者証明書に基づいて、前記被証明情報の正当性を確認する

ことを特徴とする請求項 5 6 に記載の情報処理装置。

【請求項 5 8】 前記被証明情報には、電子署名が含まれており、
前記確認手段は、前記電子署名に基づいて、前記被証明情報の正当性を確認する。

ことを特徴とする請求項 5 6 に記載の情報処理装置。

【請求項 5 9】 前記被証明情報には、前記公開鍵に対応する秘密鍵によって生成された電子署名が含まれており、

前記確認手段は、前記電子署名を、前記公開鍵で処理することにより、前記被証明情報の正当性を確認する

ことを特徴とする請求項 5 7 に記載の情報処理装置。

【請求項 6 0】 それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データと、

前記秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、前記有効性データによって、その有効性が証明される被証明情報と

からなる情報セットを検査する情報処理方法において、

他の装置からの前記被証明情報を受信する被証明情報受信ステップと、

前記他の装置からの前記秘密情報の存在を証明する証明データを受信する証明データ受信ステップと、

前記証明データと、前記被証明情報に含まれる検証用パラメータとを用いて、前記他の装置における前記秘密情報の存否を判定する存否判定ステップと

を備えることを特徴とする情報処理方法。

【請求項 6 1】 それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データと、

前記秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、前記有効性データによって、その有効性が証明される被証明情報と

からなる情報セットを検査する処理を、コンピュータに行わせるプログラムが記録されているプログラム記録媒体において、

他の装置からの前記被証明情報を受信する被証明情報受信ステップと、

前記他の装置からの前記秘密情報の存在を証明する証明データを受信する証明データ受信ステップと、

前記証明データと、前記被証明情報に含まれる検証用パラメータとを用いて、前記他の装置における前記秘密情報の存否を判定する存否判定ステップとを備えるプログラムが記録されていることを特徴とするプログラム記録媒体。

【請求項 6 2】 第 1 乃至第 3 の情報処理装置から構成される情報処理システムにおいて、

前記第 1 の情報処理装置は、

それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データを生成する有効性データ生成手段と、

前記秘密情報が存在することを検証するのに用いられる検証用パラメータを生成する検証用パラメータ生成手段と、

前記検証用パラメータを含み、前記有効性データによって、その有効性が証明される被証明情報を生成する被証明情報生成手段と、

前記有効性データと被証明情報とからなる情報セットを外部に出力する出力手段と

を備え、

前記第 2 の情報処理装置は、

前記情報セットを記憶する記憶手段と、

前記被証明情報を、その被証明情報を検査する前記第 3 の情報処理装置に送信する被証明情報送信手段と、

前記秘密情報の存在を証明する証明データを生成し、前記第 3 の情報処理装置に送信する証明データ生成手段と

を備え、

前記第 3 の情報処理装置は、

前記第 2 の情報処理装置からの前記被証明情報を受信する被証明情報受信手段と、

前記第 2 の情報処理装置からの前記秘密情報の存在を証明する証明データを受信する証明データ受信手段と、

前記証明データと、前記被証明情報に含まれる検証用パラメータとを用いて、前記第 2 の情報処理装置における前記秘密情報の存否を判定する存否判定手段とを備える

ことを特徴とする情報処理システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報記録媒体、情報処理装置および情報処理方法、プログラム記録媒体、並びに情報処理システムに関し、特に、例えば、利便性の高い電子チケットを実現することができるようにする情報記録媒体、情報処理装置および情報処理方法、プログラム記録媒体、並びに情報処理システムに関する。

【0002】

【従来の技術】

例えば、乗車券、入場券、予約券、会員書、許可書、サービス券などは、それを所持する者が、そこに記されている権利を有することを証明する。

【0003】

いま、このように、それを所持する者が有する権利を証明するものを、チケットと呼ぶこととすると、紙（紙に類するプラスチック等も含む）によるチケットは、携帯に便利な大きさの紙等に、所定事項を印刷することで実現されることから、携帯に便利であるという「携帯性」を有する。

【0004】

また、紙によるチケットを、単なる印刷を行って実現した場合には、偽造等を防止することが困難である。そこで、従来より、偽造等を防止するための手段として、例えば、特殊な印刷や、検印、あるいは透かしが付された紙などが用いられている。従って、紙によるチケットは、正当な発行者のみが発行でき、容易には偽造できないという「複製防止機能」を有する。

【0005】

さらに、紙によるチケットは、それを所持するものが有する権利を証明する「権利証明機能」や、チケット自体を譲渡することで、第三者に、そのチケットに基づく権利を容易に譲渡することができるという「譲渡性」を有する。

【0006】

ところで、従来より、電話網やコンピュータネットワークを経由してチケットの取得の予約手続きを行うことが可能であったが、チケットの最終的な受け取りは、郵送あるいは手渡しによって行われており、従って、ユーザは、チケットの受け取りのために、店舗に出向く等の必要があった。

【0007】

そこで、最近では、コンピュータネットワーク技術の進歩に伴い、チケットを電子情報化し、チケット自体を通信回線を介してやり取りする電子チケットシステムの研究、開発が行われている。いま、このように電子情報化されたチケットを、電子チケットと呼ぶこととすると、電子チケットによれば、ユーザは、その受け取りのために、店舗等に出向く必要がなくなり、さらには、チケットの流通コストおよび管理コストを削減すること等が可能となる。

【0008】

電子チケットシステムを実現する方法としては、例えば、特開平8-147500号公報等に開示されているような第1の方法や、特開平11-31204号公報等に開示されているような第2の方法が提案されている。

【0009】

即ち、第1の方法では、電子チケットの実体である電子チケット情報が複製されることにより、電子チケットに基づく権利を多重利用（行使）することができないように、電子チケット情報が、耐タンパー(tamper)性のあるハードウェアによって保持される。

【0010】

そして、電子チケットによってサービスの提供を受ける場合等においては、その電子チケット情報を保持している保持装置と、その電子チケット情報を検査する検査装置との間で、お互いが、電子チケットシステムの正当な参加機器であることを確認する認証が、例えば、検査装置が保持装置に対して特別の命令を送り

、暗号化の技術等を用いることによって行われる。この認証によって、保持装置と検査装置とが、互いに正当な機器であることが確認されると、保持装置から検査装置に対して、保持装置が記憶している電子チケット情報が送信される。

【0011】

以上のように、第1の方法では、電子チケット情報をやりとりする保持装置と検査装置とが、正当な機器であることを確認することによって、正当な機器以外の機器に、電子チケット情報が、不正に漏洩することを防止するようになっている。

【0012】

従って、第1の方法によれば、電子チケットに基づく権利を有していることの証明、即ち、権利証明を行うために、相手が正当な機器であるかどうかを確認しなければならず、紙によるチケットに比較して不便である。

【0013】

即ち、紙によるチケットであれば、そのチケットを相手に提示することによって、容易かつ安全に、つまり、相手が誰であるかを確認せずに、かつ、チケットに基づく権利が不正に取得されることを心配することなく、権利証明を行うことができる。しかしながら、第1の方法では、相手を確認し、しかも、権利を証明する電子チケット情報を相手に渡さないと、権利証明を行うことができない。

【0014】

そこで、第2の方法では、電子チケット情報自体をやりとりするのではなく、電子チケット情報を用いて、所定の処理を行い、その処理結果をやりとりすることによって、権利証明を行うことが可能となっている。

【0015】

即ち、第2の方法では、認証方法として用いられることが多い、いわゆるチャレンジアンドレスポンス(Challenge & Response)の手法を利用して、権利証明が行われる。

【0016】

具体的には、まず、電子チケットを検査する検査装置が、乱数を発生し、電子チケット情報を保持する保持装置に送信する。保持装置は、検査装置からの乱数

を受信し、その乱数を、電子チケット情報に含まれる秘密の情報を用いて処理し、その処理結果を、検査装置に送信する。検査装置は、保持装置からの処理結果を、公開された情報を用いて処理し、その処理結果と、保持装置に送信した乱数とに基づいて、電子チケットが正当なものであるかどうかを確認（検査）する。

【0017】

このようなチャレンジアンドレスポンスは、例えば、いわゆる電子署名を用いて行われ、この場合、電子チケット情報に含まれる秘密の情報は、公開鍵暗号化方式の秘密鍵となり、また、検査装置で用いられる公開された情報は、その秘密鍵に対応する公開鍵となる。そして、保持装置では、検査装置からの乱数（チャレンジ）を、秘密鍵を用いて処理することで、電子署名が作成され、検査装置では、その電子署名（レスポンス）を、公開鍵を用いて処理することにより、その電子署名と、元の乱数との対応が検証される。

【0018】

以上のような第2の方法によれば、電子チケット情報に含まれる秘密の情報としての秘密鍵は、保持装置の外部に示される公開された情報としての公開鍵から認識することはできず、さらに、チャレンジアンドレスポンスの処理過程において、外部に漏洩することがない。従って、電子チケットの権利証明を、紙によるチケットの場合と同様に、容易かつ安全に、第三者に対して行うことができる。

【0019】

【発明が解決しようとする課題】

ところで、上述の特開平11-31204号公報においては、電子チケットの必要機能として、以下の3つの点が挙げられている。

【0020】

即ち、第1点は、複製等によって正当な権利を持たないものにチケットを利用されることを防ぐ機能である「権利複製防止」であり、第2点は、身元などが特定されない匿名の者をも含む第三者に対して、電子チケットに基づく権利を証明する機能である「権利証明」であり、第3点は、電子チケットを利用する際（電子チケットに基づく権利を行使して、サービスの提供を受ける際）に、その利用者の匿名性を保証する機能である「匿名性」である。

【0021】

これらの第1乃至第3点は、いずれも従来の紙によるチケットにおいて実現されている機能であり、電子チケットにおいても、紙によるチケットの利便性を損なわないように維持されるべきものである。

【0022】

しかしながら、電子チケットにおいて、紙によるチケットと同様の利便性を確保するには、上述の3つの機能だけでは足りず、以下の、第4および第5の機能が必要であると考えられる。

【0023】

即ち、第4点としては、電子チケットに基づく権利を他人に譲ることができる機能である「譲渡性」が必要であると考えられる。さらに、第5点としては、電子チケットの権利確認のために、つまり、「権利証明」を行うために、チケット管理センタや、管理データベース等へのアクセスをその都度必要とはしないという「完結性」が必要であると考えられる。

【0024】

紙によるチケットは、それ自体を、他人に渡すことで、そのチケットに基づく権利を、他人に譲ることができる。従って、「譲渡性」は、紙によるチケットと同様の利便性を確保するために、必要不可欠の機能である。

【0025】

また、例えば、鉄道駅やイベントの入場改札等においては、紙によるチケットの提示や受け渡し等によって、そのチケットに基づく権利を、即座に確認し、円滑な入場整理を行うことができる。従って、改札等において、例えば、クレジットカードのようなオンライン検査を必要としたり、あるいは、ある番号のチケットが何を意味するかをデータベースの一覧表から検索することを必要とするのでは、円滑な入場が妨げられることになり、「権利証明」を、電子チケットそれ自体で行うことのできる「完結性」は、電子チケットの現実的な利用を考えた場合には不可欠なものとなる。

【0026】

しかしながら、上述の第2の方法では、「譲渡性」および「完結性」を満足す

ることは困難である。

【0027】

即ち、第2の方法では、電子チケット（としての情報）は、個々の電子チケットごとに異なる特徴情報（例えば、上述の公開鍵暗号化方式の秘密鍵）を、個々の保持装置ごとに異なる暗号鍵で暗号化することにより発行される。さらに、第2の方法では、保持装置が保持している暗号化された特徴情報を、その保持装置が保持している暗号鍵でしか復号することができないようにして、「権利複製防止」を実現している。そして、第2の方法において、電子チケットについての「権利証明」は、保持装置が保持している暗号化された特徴情報を、その保持装置が保持している暗号鍵で復号し、その復号した特徴情報を用いて行われる。

【0028】

以上から、第2の方法では、電子チケットが発行された保持装置でしか、その電子チケットの特徴情報を復号することができず、その結果、電子チケットが発行された保持装置以外の保持装置では、「権利証明」を行うことができない。このことは、ある保持装置に発行された電子チケットを、他の保持装置に譲ることができないこと、つまり、「譲渡性」に欠けることを意味する。

【0029】

また、紙によるチケットは、そのチケットとしての紙に書かれている内容である「権利条項」と、印刷、材質、検印、透かしなどによって偽造および複製が困難な紙自体が表すチケットの「有効性」の2つの要素を有していると考えることができ、この「権利条項」と「有効性」は、印刷によって密接不可分に結びついている。つまり、「権利条項」自体は情報であるが、その「権利条項」が印刷された複製等の困難な紙という「有効性」があって、はじめて、チケットたり得る。

【0030】

紙によるチケットは、「有効性」と「権利条項」の両方を、密接不可分に組み合わせたものとなっており、これによって、「権利複製防止」、「権利証明」、「匿名性」、「譲渡性」、および「完結性」の5つの機能が実現されている。

【0031】

紙によるチケットが備える「有効性」と「権利条項」のうち、特に、「有効性

」については、紙によるチケットが有する特徴を維持したまま電子情報化するのが困難であり、このため、第2の方法では、紙によるチケットの「有効性」の特徴であるポータビリティ(portability)を犠牲にすることで、「権利複製防止」を実現している。つまり、第2の方法では、電子チケットの「有効性」を、特定の保持装置の存在と結び付け、「譲渡性」を犠牲にして、「権利複製防止」を実現している。

【 0 0 3 2 】

さらに、第2の方法では、「権利証明」において、上述のようなチャレンジアンドレスポンスの認証方法が用いられるが、その際、検査装置は、自身が発生した乱数に対する電子署名を生成するのに用いる秘密鍵を識別する識別番号を、保持装置に送信する。保持装置においては、上述のように、電子チケットごとに異なる特徴情報としての秘密鍵が、保持装置ごとに異なる暗号鍵で暗号化されており、保持装置は、検査装置から、識別番号を受信すると、その識別番号に対応する秘密鍵を検索する。そして、保持装置は、その秘密鍵を、保持装置に固有の暗号鍵で復号し、その秘密鍵で、検査装置からの乱数を処理することによって、電子署名を生成する。この電子署名は、保持装置から検査装置に送信され、検査装置は、その電子署名を、保持装置に送信した識別番号によって特定される秘密鍵に対応する公開鍵で処理する。そして、検査装置は、その処理結果に基づいて、電子署名の検証を行い、電子チケットに基づく権利の確認(検査)を行う。

【 0 0 3 3 】

このように、第2の方法では、チャレンジアンドレスポンスの認証方法を用いることによって、電子チケットに基づく権利を表す秘密鍵を外部に示すことなく、紙によるチケットと同様の安全な権利確認(「権利証明」)を行うことができる。

【 0 0 3 4 】

しかしながら、第2の方法では、電子チケットに基づく権利を、どのように確認(検証)するべきかという情報、つまり、上述の場合には、ある電子チケットに基づく権利を、チャレンジアンドレスポンスの認証方法によって確認するのに必要な情報は、電子チケットの情報とは別に用意されており、検査装置側で把握

しなければならない。

【0035】

即ち、第2の方法においては、例えば、ある電子チケットに基づく権利を表す秘密鍵に対応する公開鍵と、その秘密鍵を識別する識別番号とが公開され、あるチケット管理センタに登録される。従って、検査装置は、ある電子チケットに基づく権利を確認する場合に、その権利を表す秘密鍵を識別する識別番号と、対応する公開鍵を、チケット管理センタにアクセスして取得する必要がある。

【0036】

検査装置が確認する権利内容が、常に同一であれば、検査装置は、チケット管理センタにアクセスして、識別番号および公開鍵を、一度だけ取得すれば問題ないが、電子チケットが普及した場合を考えると、検査装置が確認する権利内容が、常に同一であることを前提とするのは非現実的である。

【0037】

即ち、例えば、鉄道の切符を、電子チケットで実現した場合を考えると、改札として機能する検査装置は、各駅において日々発行され、さらには、普通電車や特急電車等によって権利内容が異なる電子チケットを検査しなければならない。従って、検査装置は、例えば、駅や、日、電車の種類ごとに異なる識別番号および公開鍵を、電子チケットの検査を行うたびに、チケット管理センタにアクセスして取得しなければならず、この場合、電子チケットの検査に時間を要することとなり、円滑な改札が妨げられることになる。これは、第2の方法において、電子チケットが、それ自体で、権利内容を確認することができるという「完結性」を欠いていることに起因する。

【0038】

さらに、この「完結性」の欠如は、「譲渡性」の実現に影響を与える。即ち、電子チケットが「完結性」を有しない場合には、電子チケットの譲渡にあたって、その電子チケットが有効であるかどうかの検査を、上述のように、チケット管理センタにアクセスして確認しなければならないこととなる。従って、電子チケットに、その譲渡を可能とする機能を、単に追加したとしても、電子チケットが「完結性」を有しなければ、電子チケットが有効であるかどうかの検査が煩雑と

なり、このことは、電子チケットの譲渡を行うにあたって障害となる。

【 0 0 3 9 】

つまり、紙によるチケットであれば、一般に、その紙によるチケットを見ることによって、即座に、そのチケットの有効性を検査（確認）することができ、極端には、どのような相手からであっても、チケットが有効であるかどうかを、即座に確認して、その譲渡を受けることができる。

【 0 0 4 0 】

しかしながら、電子チケットが「完結性」を有しない場合には、譲渡にあたって、電子チケットが有効であるかどうかの検査を即座に行うことができず、電子チケットが、譲渡可能な機能を有していても、事実上、譲渡が行われないこととなる。即ち、電子チケットの譲渡が行われるのは、實際上、電子チケットの発行者から、ユーザに対してだけということになる。

【 0 0 4 1 】

本発明は、このような状況に鑑みてなされたものであり、「権利複製防止」、「権利証明」、および「匿名性」の他に、「譲渡性」および「完結性」をも有する、利便性の高い電子チケットを実現することができるようにするものである。

【 0 0 4 2 】

【課題を解決するための手段】

本発明の情報記録媒体は、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データと、秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報とが記録されていることを特徴とする。

【 0 0 4 3 】

本発明の第 1 の情報処理装置は、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データを生成する有効性データ生成手段と、秘密情報が存在することを検証するのに用いられる検証用パラメータを生成する検証用パラメータ生成手段と、検証用パラメータを含み、有効性データによって

、その有効性が証明される被証明情報を生成する被証明情報生成手段と、有効性データと被証明情報とからなる情報セットを外部に出力する出力手段とを備えることを特徴とする。

【 0 0 4 4 】

本発明の第 1 の情報処理方法は、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データを生成する有効性データ生成ステップと、秘密情報が存在することを検証するのに用いられる検証用パラメータを生成する検証用パラメータ生成ステップと、検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報を生成する被証明情報生成ステップと、有効性データと被証明情報とからなる情報セットを外部に出力する出力ステップとを備えることを特徴とする。

【 0 0 4 5 】

本発明の第 1 のプログラム記録媒体は、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データを生成する有効性データ生成ステップと、秘密情報が存在することを検証するのに用いられる検証用パラメータを生成する検証用パラメータ生成ステップと、検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報を生成する被証明情報生成ステップと、有効性データと被証明情報とからなる情報セットを外部に出力する出力ステップとを備えるプログラムが記録されていることを特徴とする。

【 0 0 4 6 】

本発明の第 2 の情報処理装置は、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含む、情報の有効性を証明するための有効性データにおける秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報を、その被証明情報を検査する検査装置に送信する被証明情報送信手段と、秘密情報の存在を証明する証明データを生成し、検査装置に送信する証明データ生成手段とを備えることを特徴とする。

【 0 0 4 7 】

本発明の第2の情報処理方法は、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含む、情報の有効性を証明するための有効性データにおける秘密情報が存在することを確認するのに用いられる検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報を、その被証明情報を検査する検査装置に送信する被証明情報送信ステップと、秘密情報の存在を証明する証明データを生成し、検査装置に送信する証明データ生成ステップとを備えることを特徴とする。

【 0 0 4 8 】

本発明の第2のプログラム媒体は、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含む、情報の有効性を証明するための有効性データにおける秘密情報が存在することを確認するのに用いられる検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報を、その被証明情報を検査する検査装置に送信する被証明情報送信ステップと、秘密情報の存在を証明する証明データを生成し、検査装置に送信する証明データ生成ステップとを備えるプログラムが記録されていることを特徴とする。

【 0 0 4 9 】

本発明の第3の情報処理装置は、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含む、情報の有効性を証明するための有効性データにおける秘密情報が存在することを確認するのに用いられる検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報を受信する被証明情報受信手段と、秘密情報の存在を証明する証明データを受信する証明データ受信手段と、証明データと、被証明情報に含まれる検証用パラメータとを用いて、他の装置における秘密情報の存否を判定する存否判定手段とを備えることを特徴とする。

【 0 0 5 0 】

本発明の第3の情報処理方法は、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含む、情

報の有効性を証明するための有効性データにおける秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報を受信する被証明情報受信ステップと、秘密情報の存在を証明する証明データを受信する証明データ受信ステップと、証明データと、被証明情報に含まれる検証用パラメータとを用いて、他の装置における秘密情報の存否を判定する存否判定ステップとを備えることを特徴とする。

【 0 0 5 1 】

本発明の第3のプログラム記録媒体は、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含む、情報の有効性を証明するための有効性データにおける秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報を受信する被証明情報受信ステップと、秘密情報の存在を証明する証明データを受信する証明データ受信ステップと、証明データと、被証明情報に含まれる検証用パラメータとを用いて、他の装置における秘密情報の存否を判定する存否判定ステップとを備えるプログラムが記録されていることを特徴とする。

【 0 0 5 2 】

本発明の情報処理システムは、第1の情報処理装置が、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データを生成する有効性データ生成手段と、秘密情報が存在することを検証するのに用いられる検証用パラメータを生成する検証用パラメータ生成手段と、検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報を生成する被証明情報生成手段と、有効性データと被証明情報とからなる情報セットを外部に出力する出力手段とを備え、第2の情報処理装置が、情報セットを記憶する記憶手段と、被証明情報を、その被証明情報を検査する第3の情報処理装置に送信する被証明情報送信手段と、秘密情報の存在を証明する証明データを生成し、第3の情報処理装置に送信する証明データ生成手段とを備え、第3の情報処理装置が、第2の情報処理装置からの被証明情報を受信する被証明情報受信手段と、第2の情報

処理装置からの秘密情報の存在を証明する証明データを受信する証明データ受信手段と、証明データと、被証明情報に含まれる検証用パラメータとを用いて、第2の情報処理装置における有効性データの存否を判定する存否判定手段とを備えることを特徴とする。

【0053】

本発明の情報記録媒体においては、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データと、秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報とが記録されている。

【0054】

本発明の第1の情報処理装置および情報処理方法、並びにプログラム記録媒体においては、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データが生成されるとともに、秘密情報が存在することを検証するのに用いられる検証用パラメータが生成される。そして、検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報が生成され、有効性データと被証明情報とからなる情報セットが発行される。

【0055】

本発明の第2の情報処理装置および情報処理方法、並びにプログラム記録媒体においては、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含む、情報の有効性を証明するための有効性データにおける秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報が、その被証明情報を検査する検査装置に送信される。さらに、秘密情報の存在を証明する証明データが生成され、検査装置に送信される。

【0056】

本発明の第3の情報処理装置および情報処理方法、並びにプログラム記録媒体においては、それ自体を外部に示すことなく、それが存在することを証明するこ

とができるアルゴリズムが適用可能な秘密情報を含む、情報の有効性を証明するための有効性データにおける秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報が受信されるとともに、秘密情報の存在を証明する証明データが受信される。そして、証明データと、被証明情報に含まれる検証用パラメータとを用いて、他の装置における秘密情報の存否が判定される。

【 0 0 5 7 】

本発明の情報処理システムにおいては、第 1 の情報処理装置において、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含む、情報の有効性を証明するための有効性データが生成されるとともに、秘密情報が存在することを検証するのに用いられる検証用パラメータが生成される。さらに、検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報が生成され、有効性データと被証明情報とからなる情報セットが発行される。第 2 の情報処理装置では、被証明情報が、その被証明情報を検査する第 3 の情報処理装置に送信されるとともに、秘密情報の存在を証明する証明データが生成され、第 3 の情報処理装置に送信される。第 3 の情報処理装置では、第 2 の情報処理装置からの被証明情報が受信されるとともに、第 2 の情報処理装置からの有効性データの存在を証明する証明データが受信され、証明データと、被証明情報に含まれる検証用パラメータとを用いて、第 2 の情報処理装置における秘密情報の存否が判定される。

【 0 0 5 8 】

【発明の実施の形態】

図 1 は、本発明を適用した電子チケットシステム（システムとは、複数の装置が論理的に集合した物をいい、各構成の装置が同一筐体中に存在するか否かは問わない）の一実施の形態の構成例を示している。

【 0 0 5 9 】

この電子チケットシステムは、チケット管理センタ 1、チケット発行者が有するチケット発行装置 $3_1, 3_2, \dots, 3_T$ 、ユーザが有するチケット保持装置 $4_1, 4_2, \dots, 4_U$ 、およびサービス提供者が有するチケット検査装置 $5_1,$

5₂, ..., 5_sが、相互に、ネットワーク 2 を介して接続されることにより構成されている。

【 0 0 6 0 】

チケット管理センタ 1 は、電子署名の認証センタとして機能する。

【 0 0 6 1 】

ネットワーク 2 は、例えば、公衆回線、インターネット、CATV (Cable Television) 網、地上波、衛星回線等で構成される。

【 0 0 6 2 】

チケット発行者が有するチケット発行装置 3_tは、電子チケット（厳密には、電子チケットの実体となる情報（電子チケット情報））を発行し、ユーザが有するチケット保持装置 4_uに提供する。

【 0 0 6 3 】

なお、チケット発行装置 3_tにおいて、電子チケットの提供は、チケット保持装置 4_uとネットワーク 2 を介して通信することにより行うことも可能であるし、チケット保持装置 4_uと直接に、無線または有線で通信することにより行うことも可能である。また、チケット保持装置 4_uのユーザは、必要に応じて、チケット発行装置 3_tに対して電子チケットの提供（譲渡）に対する対価として、その電子チケットの代金を支払う。この電子チケットの代金の支払いのための課金処理は、ネットワーク 2 を介して行うことも可能であるし、チケット発行装置 3_tとチケット保持装置 4_uとの間で、直接に通信することによって行うことも可能である。さらに、電子チケットの代金の支払いは、その代金を、チケット発行装置 3_tに直接投入して行うことも可能である。

【 0 0 6 4 】

ユーザが有するチケット保持装置 4_uは、チケット発行装置 3_tが発行する電子チケット（の実体である電子チケット情報）を保持する。ユーザは、このチケット保持装置 4_uが保持する電子チケットに基づく権利を行使することができ、これにより、チケット検査装置 5_sを有するサービス提供者（チケット発行装置 3_tを有するチケット発行者と同一である場合もある）から、その権利に対応するサービスの提供を受けることができる。

【 0 0 6 5 】

なお、ユーザは、チケット保持装置 4_u どうしの間で通信を行うことにより、電子チケット（に基づく権利）を授受することができる。この電子チケットの授受は、電子チケットが使用される前に行うことができる他、電子チケットが、有効期限や使用回数の制限のあるものである場合には、使用された後であっても、有効期限が切れる前や、使用回数の制限を越える前であれば行うことができる。また、チケット保持装置 4_u は、有効期限が切れた電子チケットや、使用回数制限を越えた電子チケット等の不要な電子チケットを破棄することができる。さらに、チケット保持装置 4_u では、複数の電子チケットを保持することができる。

【 0 0 6 6 】

サービス提供者が有するチケット検査装置 5_s は、チケット保持装置 4_u が保持する電子チケットの検査（検証）を行う。なお、電子チケットの検査も、チケット発行装置 3_t からチケット保持装置 4_u に対する電子チケットの提供（譲渡）と同様に、ネットワーク 2 を介して行うことも可能であるし、チケット保持装置 4_u とチケット検査装置 5_s との間で、直接通信することによって行うことも可能である。

【 0 0 6 7 】

なお、チケット管理センタ 1、チケット発行装置 3_t、チケット保持装置 4_u、およびチケット検査装置 5_s は、いずれも、例えば、コンピュータで構成することが可能である。また、例えば、チケット保持装置 4_u は、IC (Integrated Circuit) カードで構成し、チケット発行装置 3_t およびチケット検査装置 5_s は、IC カードのリーダー/ライターで構成することも可能である。さらに、チケット保持装置 4_u は、例えば、携帯電話機や、PDA (Personal Digital Assistant) 等の携帯端末で構成することも可能である。

【 0 0 6 8 】

以上のように構成される電子チケットシステムにおいては、上述の「権利複製防止」、「権利証明」、「匿名性」、「譲渡性」、および「完結性」の 5 つの機能すべてを有する電子チケットを流通させることができるようになっている。

【 0 0 6 9 】

即ち、図1の電子チケットシステムで対象とする電子チケットは、複製できないが、移動が可能な「有効性」と、それに結びついた「権利条項」とから構成され、さらに、個々の電子チケットは、それぞれ異なる「有効性」を有する。

【0070】

電子チケットの「有効性」を表す情報は、例えば、電子署名を生成するのに用いられる情報（例えば、公開鍵暗号化方式の秘密鍵、ゼロ知識証明の可能な情報など）などの、認証によってその存在が確認できるが、それ自体は外部に漏れない（示されない）性質を有する情報（秘密情報）と、後述する付加情報とから構成される。

【0071】

「有効性」を表す情報は、チケット保持装置4_uにおいて、後述する手法により、複製や改竄をすることができないように保持される。また、「有効性」を表す情報は、そのチケット保持装置4_uを有するユーザでさえも知ることができない。

【0072】

「権利条項」を表す情報は、従来の紙によるチケットに書かれている情報に相当する。従って、電子チケットが、例えば、イベントチケットの場合には、「権利条項」を表す情報は、開催日時や、場所、イベント名などから構成される。但し、電子チケットにおいては、「権利条項」を表す情報には、「有効性」を表す情報の存在を検証するのに用いられるパラメータ（検証用パラメータ）も含まれる。即ち、例えば、「有効性」を表す情報が、電子署名を生成するのに用いられる公開鍵暗号化方式の秘密鍵である場合には、「権利条項」を表す情報には、その秘密鍵に対応する公開鍵が含まれる。

【0073】

さらに、「権利条項」を表す情報には、その電子チケットのチケット発行者の証明書（後述する発行者証明書）と、チケット発行者による電子署名とが含まれる。ここで、「権利条項」に含まれるチケット発行者の証明書は、電子チケットのチケット発行者と、「有効性」の存在を検証するのに用いられる公開鍵との対応を証明し、これにより、「権利条項」の改竄を防止するとともに、「権利条項

」と、対応する「有効性」との関係を変更することを防止する。

【0074】

電子チケットを構成する「権利条項」は、上述のように、紙によるチケットに書かれている情報に相当し、それ自体は、電子チケットに基づく権利の内容を表すものであるが、電子チケットとしての正当性（有効性）を証明するには、「有効性」の存在が必要となる。そして、「有効性」を表す情報は、上述のように、その存在を証明するにあたって、外部に示されない。

【0075】

従って、電子チケットに基づく権利の内容は、「権利条項」を示す（出力すること）で、任意の第三者に認識させることができ、さらに、その権利が有効なものかどうかは、外部には示されない「有効性」の存在によって証明されるから、「権利条項」を表す情報自体は、仮に、悪意の第三者に複製されたとしても、「有効性」が存在しない限り、電子チケットが複製されたことにはならない。その結果、「権利条項」を表す情報は、第三者による複製を心配せずに扱うことができる。

【0076】

以上のような「有効性」と「権利条項」の組からなる電子チケットを実現するために、チケット管理センタ1は、チケット発行者の証明書（発行者証明書）を発行する認証センタとして機能する。

【0077】

即ち、チケット管理センタ1は、電子署名を生成する秘密鍵としての署名生成用秘密鍵 S_{CA} と、その秘密鍵に対応する公開鍵としての署名検証用公開鍵 P_{CA} を有している。署名生成用秘密鍵 S_{CA} は、外部には一切秘密にされ、署名検証用公開鍵 P_{CA} は、ネットワーク2を介して、誰でも取得することができるように公開される。

【0078】

そして、チケット管理センタ1は、署名生成用秘密鍵 S_{CA} を用いて、発行者証明書を生成し、チケット発行者に対して発行する。このように、発行者証明書は、チケット管理センタ1だけが知り得る署名生成用秘密鍵 S_{CA} を用いて生成され

るため、チケット管理センタ1だけが発行することができる。この発行者証明書と、後述するチケット発行者の署名によって、チケット発行者以外の者が、そのチケット発行者が発行した電子チケットを改竄することが防止される。

【0079】

電子チケットについては、「発行」、「行使」、「譲渡」、および「破棄」の4つの操作が可能となっている。

【0080】

電子チケットの「発行」は、チケット発行装置3_tで行われるが、その発行時に、電子チケットを所有する者（チケット保持装置4_u）を特定する情報を、電子チケットに含める必要はない。その結果、チケット発行装置3_tが発行し、あるチケット保持装置4_uに譲渡した電子チケットは、「譲渡」によって、そのチケット保持装置4_uから他のチケット保持装置4_uに移動することができる。つまり、紙によるチケットにおける場合と同様に、電子チケットを譲渡することができる。

【0081】

電子チケット（に基づく権利）の「行使」は、チケット保持装置4_uから、電子チケットの「権利条項」の情報を、サービス提供者のチケット検査装置5_sに出力し、さらに、チケット検査装置5_sに対して、その「権利条項」の情報の有効性を証明する「有効性」の情報が、チケット保持装置4_uに存在することを証明することによって行われる。

【0082】

即ち、チケット検査装置5_sは、チケット保持装置4_uからの「権利条項」の情報の正当性（改竄されていないかどうか）を確認し、それに対応するサービスを提供することができるのであれば、その「権利条項」の情報、つまりは電子チケット自体の有効性を証明する「有効性」の情報がチケット保持装置4_uに存在するかどうかの確認を行う。

【0083】

「有効性」の情報が存在することの確認は、チケット保持装置4_uから見れば、「権利証明」を行うことになる。この「権利証明」は、例えば、チャレンジア

ンドレスポンスの認証方法によって行われる。即ち、チケット検査装置 5_s は、チケット保持装置 4_u に乱数を送信し、チケット保持装置 4_u は、その乱数から、「有効性」の情報を用いて、電子署名を生成し、チケット検査装置 5_s に返す。チケット検査装置 5_s は、チケット保持装置 4_u からの電子署名と、元の乱数との一致性を判断することにより、電子署名の認証を行う。そして、チケット検査装置 5_s は、その認証が成功すれば、チケット保持装置 4_u に「権利条項」の情報に対応する「有効性」の情報が存在するとして、即ち、そのチケット保持装置 4_u が保持している電子チケットが有効であるとして、その電子チケットに基づく権利の行使を認める。これにより、サービス提供者は、チケット保持装置 4_u のユーザに対して、所定のサービスを提供する。

【 0 0 8 4 】

このように、「権利証明」は、チャレンジアンドレスポンスの認証方法によって行われるため、「有効性」の情報は、チケット保持装置 4_u の外部に漏れることはない。従って、「権利証明」を、不特定の第三者に対して、電子チケットに基づく権利を安全に保ちながら（複製を防止し、さらには、盗まれる心配をせずに）行うことができる。

【 0 0 8 5 】

ここで、紙によるチケットには、大きく分けて、権利証明書として何回でも反復使用ができるものと、乗車券、回数券等のように使用回数が制限されるもの、あるいは定期券などのように使用期間が限定されるものとの2種類が存在する。

【 0 0 8 6 】

電子チケットにおいても、紙によるチケットと同様に、反復使用ができるものと、使用回数または使用期間が限定されているものの2種類の実現が可能である。

【 0 0 8 7 】

即ち、例えば、使用回数が限定された電子チケットは、その電子チケットの使用回数と、その使用回数の制限値とを、電子チケットに含めることにより実現することが可能である。そして、サービス提供者において、チケット検査装置 4_s によって、電子チケットの使用回数とその制限値とを比較し、使用回数が制限値

を越えている場合には、サービスの提供を拒否すれば良い。

【0088】

なお、この場合、使用回数が限定された電子チケットについて、使用回数が制限値を越えているときには、その電子チケットを無効とする必要があるが、そのためには、使用回数が制限値を越えているかどうかを判断する必要がある。従って、使用回数および制限値は、その改竄をすることができないように、電子チケットに書き込む必要がある。

【0089】

また、使用期限が制限された電子チケットも、その使用期限を電子チケットに含めることで実現することが可能である。

【0090】

ところで、例えば、新幹線の特急券を、電子チケットで実現する場合を考えてみると、一度使用を開始した特急券を使用して、別の新幹線に乗車することを制限する他、その電子チケットで乗車した新幹線において、新幹線に乗車することの権利を証明するのに、特急券を車掌等に提示できることが必要である。

【0091】

従って、電子チケットについては、その使用回数の制限値は勿論、その使用回数、あるいは、電子チケットを使用したかどうか（電子チケットに基づく権利を行使したかどうか）を、サービス検査装置 5_s が認識することができることが重要である。

【0092】

そこで、ここでは、電子チケットに基づく権利の行使、即ち、チケット保持装置 4_u 側からすれば「権利証明」を、2つの方法によって行うことが可能となっている。

【0093】

即ち、第1の「権利証明」の方法は、上述したように、チケット保持装置 4_u に「有効性」の情報が存在することだけを証明することによる、いわば「通常の権利証明」であり、第2の「権利証明」の方法は、チケット保持装置 4_u に「有効性」の情報が存在することと、使用回数とを証明することによる、いわば「回

数付き権利証明」である。

【0094】

「回数付き権利証明」も、基本的には、「通常の権利証明」と同様に、チャレンジアンドレスポンスの認証方法によって行うことができる。但し、「回数付き権利証明」を行う場合には、チケット保持装置 4_u は、チケット検査装置 5_t から送信されてくる乱数だけではなく、その乱数と、電子チケットに含まれる使用回数との組に対して、電子署名を生成し、その電子署名と使用回数との組を、チケット検査装置 5_s に返す。チケット検査装置 5_s は、チケット保持装置 4_u からの電子署名と使用回数を用いて、「有効性」の情報の存在と、使用回数とを確認する。

【0095】

なお、「通常権利証明」と「回数付き権利証明」のうちのいずれを行うかは、例えば、ユーザが、チケット保持装置 4_u を操作することによって決定することができる。

【0096】

次に、電子チケットの「譲渡」については、あるチケット保持装置 4_u （あるいは、チケット発行装置 3_t ）が有する電子チケットを構成する「有効性」と「権利条項」の両方の情報を、他のチケット保持装置 4_u に移動することによって行われる。なお、「有効性」の情報は、譲渡側の装置と譲受側の装置との間で唯一性を保ちながら移動される。即ち、「有効性」の情報は、その移動途中で複製されないように移動される。

【0097】

電子チケットの「破棄」については、「有効性」と「権利条項」の両方の情報を削除することで実現される。なお、この「破棄」は、電子チケットを譲渡した場合に、その譲渡側の装置で行われる他、電子チケットを保持しているチケット保持装置 4_u やチケット発行装置 3_t において、例えば、有効期限や使用回数の制限値から、電子チケットが無効になったことが判明した場合も行われる。

【0098】

ところで、電子チケットにおける電子化された「有効性」の情報は、紙による

チケットが有する「有効性」と比較して、複製が容易である。

【0099】

電子チケットの「行使」においては、チャレンジアンドレスポンスの認証方法を用いることで、「有効性」の情報の存在を、その情報自体を外部に示すことなく証明することができるから、「権利証明」を行う際に、「有効性」の情報が複製されることは防止することができる。

【0100】

しかしながら、「有効性」の情報の複製は、「権利証明」時だけでなく、電子チケットがチケット保持装置4_uに保持されている状態、および電子チケットの譲渡に際し、「有効性」の情報が移動中の状態においても防止する必要がある。

【0101】

このような「有効性」の情報の複製の防止は、電子チケットの利便性を考慮すれば、パーソナルコンピュータ等の汎用の情報処理装置であっても、最小限の機能追加で行うことができるのが望ましい。

【0102】

最近では、音楽情報のネットワーク配信の普及に伴い、音楽情報を複製されないように移動し、保持するための技術が提案されている。従って、電子チケットにおける「有効性」の情報についても、この技術を取り入れて、その複製を防止することが可能である。

【0103】

即ち、音楽情報は、例えば、MP3(MPEG(Moving Picture Expert Group)1 Audio Layer 3)やATRAC(Adaptive TRAnsform Acoustic Coding)等といった汎用的な音楽情報圧縮形式に圧縮されるが、このように圧縮された音楽情報を複製することができた場合には、それを伸長して、容易に利用することができる。このため、音楽情報等(以下、コンテンツという)は、暗号化などの手法を用いて処理され、これにより、移動時や保持時において、仮に、その複製が行われたとしても、それを利用することができないようにすることで、結果として、不正な複製が防止されるようになっている。

【0104】

このように、コンテンツを不正な複製から保護する方法としては、例えば、特開平11-328850号公報に記載されているように、暗号化されたコンテンツ、その暗号を復号するコンテンツ鍵、およびコンテンツを保持する装置に固有の固有鍵を管理するハードウェアである管理回路を用いるものがある。この方法では、コンテンツは、暗号化して保持され、そのまま読み出しても利用できないものとされる。さらに、コンテンツ鍵は、固有鍵によって暗号化され、管理回路に保持されており、コンテンツを復号するときのみ、固有鍵を用いて復号される。また、コンテンツの移動は、盗聴を避けるために暗号化された状態で行われ、コンテンツの移動が行われた場合には、移動元の装置におけるコンテンツは、管理回路によって確実に削除される。管理回路は、いわゆる耐タンパー性を有し、これにより、管理回路が保持する鍵の取り出しや改竄が防止されるようになっている。

【0105】

以上のように、コンテンツを保護しながら取り扱うことが可能な実用システムとしては、例えば、本件出願人が開発したMagic Gateシステム等がある。

【0106】

電子チケットの「有効性」の情報について、唯一性を維持するには、上述のような、コンテンツを、その複製を防止しながら保持および移動する方法を利用することができる。「有効性」の情報は、音楽情報等のコンテンツに比べて、サイズが小さく、また、固定サイズとすることが可能であり、処理が容易である。さらに、「有効性」の情報を復号するのは、「権利証明」を行うときに限られるから、その盗聴や改竄を防止するのも、コンテンツに比較して容易である。また、電子チケットを保持する装置において、管理回路と、「権利証明」のための電子署名を生成する回路とを、ハードウェア的に一体に構成すること等によって、復号された「有効性」の情報の漏洩を比較的容易に防止することができる。従って、「有効性」の情報は、復号後のデータを、他の装置に移動して処理することがあるコンテンツに比較して有利である。

【0107】

以上のように、図1の電子チケットシステムにおいて流通する電子チケットは、一対一の対応関係にある「有効性」と「権利条項」の情報から構成され、その

うちの「有効性」の情報の唯一性を、チケット保持装置4_uのハードウェア機能等を利用して維持することによって、第1点の「権利複製防止」を実現することができる。さらに、「有効性」の情報の存在を示す仕組みによって、第2点の「権利証明」を行うことが可能であり、その際、チケット保持装置4_uを特定する情報を必要としないことによって、第3点の「匿名性」を実現することができる。そして、「有効性」の情報を、その唯一性を保ちながら移動することによって、第4点の「譲渡性」を実現することができる。さらに、「権利条項」の情報に、十分な情報を含ませ、かつ「権利証明」の機能を利用することによって、第5点の「完結性」を実現することが可能となる。

【0108】

次に、図2および図3を参照して、図1のチケット管理センタ1の役割について説明する。

【0109】

チケット管理センタ1は、上述したように、電子署名の認証センタとして機能する。

【0110】

即ち、チケット管理センタ1は、例えば、公開鍵暗号化方式を利用して、電子署名付きの証明書を発行する。

【0111】

ここで、公開鍵暗号化方式は非対称暗号化方式とも呼ばれ、データを暗号化する際に用いられる鍵と、その暗号を復号する際に用いられる鍵が異なり、さらに、一方の鍵から他方の鍵を算出することが非常に困難であるという性質を持った暗号アルゴリズムである。一般に、暗号化の鍵は、第三者に公開されることから公開鍵と呼ばれ、復号の鍵は、第三者に秘密にされることから秘密鍵と呼ばれる。

【0112】

公開鍵暗号化方式によれば、秘密鍵が知られない限り、その秘密鍵に対応する公開鍵や、公開鍵で暗号化されたデータ（暗号）が知られたとしても、元のデータ（公開鍵で暗号化される前のデータ）を得ることはできない。このような公開

鍵暗号化方式としては、例えば、RSA(R. L. Rivest, A. Shamir, L. Adleman)暗号、楕円曲線暗号などが知られている。

【 0 1 1 3 】

いま、あるユーザ # u に割り当てられた公開鍵と秘密鍵を、それぞれを P_u と S_u として、公開鍵 P_u によるデータ M の暗号化を、 $C=E(P_u, M)$ と表すとともに、秘密鍵 S_u による暗号 C の復号を、 $M=D(S_u, C)$ と表すこととする。

【 0 1 1 4 】

電子署名は、データを作成したユーザ # u が、そのデータを、自分の秘密鍵 S_u で復号処理することによって生成される。即ち、データ M を作成したユーザ # u は、自分の秘密鍵 S_u を用いて、式 $SG(M)=D(S_u, h(M))$ を計算し、この計算結果 $SG(M)$ が電子署名となる。

【 0 1 1 5 】

ここで、 $h()$ は一方向性関数（ハッシュ関数）であり、出力値から入力値を知ることが非常に困難であるという性質を有する。一方向性関数としては、例えば、MD5(Message Digest 5)やSHA-1(Secure Hashing Algorithm 1)などが知られている。

【 0 1 1 6 】

ユーザ # u は、データ M を、そのデータ M と電子署名 $SG(M)$ とのデータセット $(M, SG(M))$ にして送信する。このデータセット $(M, SG(M))$ を受信した受信側では、ユーザ # u の公開されている公開鍵 P_u を用いて、データセット $(M, SG(M))$ における電子署名 $SG(M)$ を暗号化処理し、その暗号化結果 $E(P_u, SG(M))$ と、データセット $(M, SG(M))$ におけるデータ M を引数として一方向性関数 $h()$ を計算した計算結果 $h(M)$ との一致性が認められるかどうか、即ち、式 $h(M)=E(P_k, SG(M))$ が満たされるかどうかを確認する。この一致性が満たされることによって、データ M が改竄されていないこと、および電子署名 $SG(M)$ が秘密鍵 S_u のユーザ # u によって付加されたことを確認することができる。電子署名としては、RSA署名やElGamal署名、楕円ElGamal署名などが知られている。

【 0 1 1 7 】

ここで、以上のようにして、データ M が改竄されていないことや、電子署名 $SG(M)$

M)が秘密鍵 S_u のユーザ# u によって付加されたことを確認することを、以下、適宜、署名確認という。また、署名確認を行うには、一方向性関数 $h()$ を知る必要があるが、以下においては、署名確認に用いられる一方向性関数 $h()$ を特定する情報は、公開鍵 P_u に含まれているものとする。

【 0 1 1 8 】

公開鍵暗号化方式によれば、以上のような署名確認を行う他、ユーザ# u が秘密鍵 S_u を所有していること（秘密鍵 S_u の存在）を、チャレンジアンドレスポンスの手法によって、秘密鍵 S_u 自体を知ることなく確認（検証）することができる。

【 0 1 1 9 】

即ち、ユーザ# u が秘密鍵 S_u を所有していることを検証する検証側は、例えば、乱数 r （チャレンジ）を発生し、その乱数 r を、ユーザ# u の公開鍵 P_u で暗号化して、暗号 $r' = E(P_u, r)$ を求める。検証側は、この暗号 r' を、ユーザ# u に送り、ユーザ# u は、暗号 r' を、秘密鍵 S_u で復号し、その復号結果 $D(S_u, r')$ （レスポンス）を、検証側に返す。検証側は、ユーザ# u からの復号結果 $D(S_u, r')$ が、自身が発生した乱数 r に等しいかどうかを判定し、等しければ、即ち、式 $r = D(S_u, r')$ が成立すれば、ユーザ# u が、秘密鍵 S_u を所有していることを確認（検証）することができる。

【 0 1 2 0 】

また、検証側では、乱数 r そのものを、ユーザ# u に送り、ユーザ# u には、その乱数 r から一方向性関数 $h()$ を計算した値 $h(r)$ を、ユーザ# u の秘密鍵 S_u で復号処理した復号処理結果 $r'' = D(S_u, h(r))$ を求めさせることができる。この場合、検証側は、その復号処理結果 r'' を、ユーザ# u の公開鍵 P_u で暗号化して、その暗号化処理結果 $E(P_u, r'')$ が、乱数 r から一方向性関数 $h()$ を計算した値 $h(r)$ に等しいかどうかを判定することで、即ち、式 $h(r) = E(P_u, r'')$ が成り立つかどうかを判定することで、ユーザ# u が、秘密鍵 S_u を所有していることを確認することができる。

【 0 1 2 1 】

なお、電子署名によっても、ユーザ# u が、電子署名を生成するための秘密鍵 S_u を所有しているかどうかを、上述の場合と同様にして、秘密鍵 S_u 自体を知るこ

となく確認することができる。即ち、検証側は、乱数 r を生成して、ユーザ $\# u$ に送信し、ユーザ $\# u$ は、乱数 r から、秘密鍵 S_u を用いて電子署名 $SG(r)=D(Sk, h(r))$ を計算して、検証側に返す。検証側は、ユーザ $\# u$ の公開鍵 P_u を用いて、電子署名 $SG(r)$ を暗号化処理し、その暗号化処理結果 $E(P_u, SG(r))$ を求める。さらに、検証側は、式 $h(r)=E(P_u, SG(r))$ が成立するかどうかを判定し、成立すれば、ユーザ $\# u$ が秘密鍵 S_u を所有していることを確認することができる。

【 0 1 2 2 】

以上のように、ユーザ $\# u$ が、特定の秘密鍵 S_u を所有していることを、その秘密鍵 S_u に対応する公開鍵 P_u を用いて確認することができるが、以下、適宜、この確認を、認証という。

【 0 1 2 3 】

署名確認や認証を行うには、その対象とする相手が所有する秘密鍵に対応する公開鍵を認識する必要がある。しかしながら、署名確認や認証を行う対象とする相手が多数の場合には、その多数の公開鍵を認識していなければならない、面倒である。そこで、ある1つの公開鍵を認識していれば、その公開鍵を用いて、他の公開鍵を連鎖的に認識することができる方法が、ITU-T(International Telecommunications Union - Telecommunications Standardization Sector)のX.509勧告において規定されている。

【 0 1 2 4 】

この認識していればよい公開鍵と、その公開鍵に対応する秘密鍵との所有者が認証センタ(CA(Certificate Authority))であり、チケット管理センタ1は、このような認証センタとして機能する。

【 0 1 2 5 】

従って、チケット管理センタ1は、自身の公開鍵と、対応する秘密鍵とを有するが、この公開鍵と秘密鍵を、それぞれ P_{CA} と S_{CA} と表す。公開鍵 P_{CA} は、広く第三者に公開されるが、秘密鍵 S_{CA} は、チケット管理センタ1以外には秘密にされる。

【 0 1 2 6 】

そして、ある所有者 $\# n$ の公開鍵と秘密鍵を、それぞれ P_n と S_n と表すと、チケ

ット管理センタ 1 は、所有者 # n から、その所有者 # n を識別する識別情報 Info_n と、公開鍵 P_n を受信し、その組 (Info_n, P_n) に対し、自身の秘密鍵 S_{CA} を用いて、電子署名 $SG_n = D(S_{CA}, h(\text{Info}_n, P_n))$ を生成する。さらに、チケット管理センタ 1 は、所有者 # n からの識別情報 Info_n および公開鍵 P_n に対して、電子署名 SG_n を付加することにより、証明書 $(\text{Info}_n, P_n, SG_n)$ を発行する。この証明書 $(\text{Info}_n, P_n, SG_n)$ は、チケット管理センタ 1 が、識別情報 Info_n で特定される所有者 # n と、その所有者 # n の公開鍵 P_n との関係を保証するものとなる。

【 0 1 2 7 】

即ち、所有者 # n は、証明書 $(\text{Info}_n, P_n, SG_n)$ を、公開鍵とその所有者との関係を検証する検証側に対して送信し、検証側は、公開されているチケット管理センタ 1 の公開鍵 P_{CA} を用い、証明書 $(\text{Info}_n, P_n, SG_n)$ の電子署名 SG_n について、署名確認を行う。これにより、証明書 $(\text{Info}_n, P_n, SG_n)$ における識別情報 Info_n と公開鍵 P_n が改竄されていないこと、即ち、証明書 $(\text{Info}_n, P_n, SG_n)$ の正当性を確認することができる。そして、証明書 $(\text{Info}_n, P_n, SG_n)$ の正当性が確認されれば、証明書 $(\text{Info}_n, P_n, SG_n)$ における識別情報 Info_n によって識別される所有者 # n が、公開鍵 P_n を所有していることを確認することができる。従って、例えば、識別情報 Info_n が人名である場合には、証明書 $(\text{Info}_n, P_n, SG_n)$ によれば、公開鍵 P_n で認証を行うことができる相手の人名 Info_n を確認することができる。

【 0 1 2 8 】

なお、証明書には、一般に、暗号化のアルゴリズムや、使用されている一方関性関数 $h()$ の種類の情報も含まれる。また、上述の場合には、チケット管理センタ 1 において、識別情報 Info_n および公開鍵 P_n の組 (Info_n, P_n) に対して、電子署名 SG_n を生成するようにしたが、公開鍵 P_n を所有する所有者 # n を確認する必要がない場合には、公開鍵 P_n に対して、電子署名 SG_n が生成され、公開鍵 P_n に、電子署名 SG_n を付加した証明書 (P_n, SG_n) が発行される。この証明書 (P_n, SG_n) は、公開鍵 P_n で認証を行うことができる相手が、認証センタであるチケット管理センタ 1 に登録されている正当なものであることを確認するのに用いることができる。

【 0 1 2 9 】

チケット発行装置 3_t は、図 2 に示すように、そのチケット発行装置 3_t を有す

るチケット発行者を識別する発行者識別情報 TID_t 、およびチケット発行者の電子署名を生成するのに用いられる秘密鍵としての発行者署名生成用秘密鍵 $TSSK_t$ と、その電子署名の署名確認（検証）に用いられる公開鍵としての発行者検証用公開鍵 $TSPK_t$ とのセットを有しており、そのうちの発行者識別情報 TID_t と発行者署名検証用公開鍵 $TSPK_t$ を、あらかじめ、チケット管理センタ 1 に送信して、登録を要求する。

【0130】

チケット管理センタ 1 は、上述のように、電子署名を生成するのに用いられる秘密鍵としての署名生成用秘密鍵 S_{CA} と、その電子署名の署名確認に用いられる公開鍵としての署名検証用公開鍵 P_{CA} を有しており、チケット発行装置 3_t からの発行者識別情報 TID_t と発行者署名検証用公開鍵 $TSPK_t$ を登録した上で、その発行者識別情報 TID_t と発行者署名検証用公開鍵 $TSPK_t$ に対して、署名生成用秘密鍵 S_{CA} を用いて電子署名 TSG_t を生成する。さらに、チケット管理センタ 1 は、チケット発行装置 3_t からの発行者識別情報 TID_t と発行者署名検証用公開鍵 $TSPK_t$ に対して、電子署名 TSG_t を付加し、これにより、発行者識別情報 TID_t によって識別されるチケット発行者と、発行者署名検証用公開鍵 $TSPK_t$ との対応関係を証明（保証）する証明書としての発行者証明書 $TP_t(=(TID_t, TSPK_t, TSG_t))$ を発行し、チケット発行装置 3_t に送信する。

【0131】

チケット発行装置 3_t は、このようにして、チケット管理センタ 1 から発行される発行者証明書 TP_t を、あらかじめ内蔵している。

【0132】

チケット保持装置 4_u には、図 3 に示すように、そのチケット保持装置 4_u が、図 1 の電子チケットシステムの正当な参加機器であることを証明するのに用いられる秘密鍵としての装置証明用秘密鍵 ASK_u と、チケット保持装置 4_u が、図 1 の電子チケットシステムの正当な参加機器であることを検証するのに用いられる公開鍵としての装置検証用公開鍵 APK_u とのセットが、あらかじめ内蔵されている。

【0133】

さらに、装置検証用公開鍵 APK_u は、あらかじめチケット管理センタ 1 に送信さ

れて登録される。また、チケット管理センタ 1 は、装置検証用公開鍵 APK_u に対して、署名生成用秘密鍵 S_{CA} を用いて電子署名 ASG_u を生成し、装置検証用公開鍵 APK_u に対して、電子署名 TSG_t を付加することにより、装置検証用公開鍵 APK_u に対応する装置証明用秘密鍵 ASK_u を有しているチケット保持装置 4_u が、正当なものであることを証明する証明書としての装置証明書 $AP_u (= (APK_u, ASG_u))$ を発行する。

【0134】

チケット保持装置 4_u は、このようにして、チケット管理センタ 1 から発行される装置証明書 AP_u を、あらかじめ内蔵している。

【0135】

次に、図 4 は、チケット発行装置 3_t が発行する電子チケットの実体としての電子チケット情報のフォーマットを示している。

【0136】

電子チケット（電子チケット情報）は、図 4（A）に示すように、チケット有効性部（「有効性」の情報）とチケット権利条項部（「権利条項」の情報）とから構成される。

【0137】

チケット有効性部は、図 4（B）に示すように、有効性証明用秘密鍵 VSK_n と付加情報とから構成される。

【0138】

有効性証明用秘密鍵 VSK_n は、それを含む電子チケット # n の有効性を証明するのに用いられる秘密鍵であり、電子チケットごとに固有の値を有する。即ち、有効性証明用秘密鍵 VSK_n は、電子チケットごとに異なる。

【0139】

なお、有効性証明用秘密鍵 VSK_n としては、例えば、公開鍵暗号化方式による暗号を復号する秘密鍵や、電子署名を生成する秘密鍵、ゼロ知識証明可能なデータ等の、データ自体は漏らさず、その存在を示すことができるデータを採用することができる。

【0140】

付加情報は、例えば、電子チケットの使用回数等で構成される。なお、この使

用回数は、電子チケットの発行時には0回に設定（初期化）される。

【0141】

チケット権利条項部は、図4（C）に示すように、チケット権利条項TI、有効性検証用公開鍵 VPK_n 、発行者証明書 TP_t 、および条項検証用署名ASGで構成される。

【0142】

チケット権利条項TIは、紙によるチケットにおける記載事項に相当し、この記載事項を参照することで、電子チケットが、どのような内容の権利を行使することができるもの（どのようなサービスを受けることができるもの）であるのかを認識することができる。即ち、例えば、電子チケットが、列車の切符であるとする、チケット権利条項TIは、例えば、乗車することのできる駅や、その乗車駅から幾ら分の区間の乗車が可能であるか、乗車可能な日等の情報から構成される。

【0143】

有効性検証用公開鍵 VPK_n は、チケット有効性部の有効性証明用秘密鍵 VSK_n に対応する公開鍵で、有効性証明用秘密鍵 VSK_n の存在を検証するのに用いられる。

【0144】

発行者証明書 TP_t は、図2で説明したように、チケット管理センタ1が、チケット発行装置3_tのチケット発行者に対して、あらかじめ発行する証明書で、上述したように、発行者識別情報 TID_t 、発行者検証用公開鍵 $TSPK_t$ 、および発行者検証用署名 TSG_t で構成される。

【0145】

条項検証用署名ASGは、チケット発行装置3_tが、チケット権利条項TI、有効性検証用公開鍵 VPK_n 、および発行者証明書 TP_t に対し、発行者署名生成用秘密鍵 $TSSK_t$ （図2）を用いて生成する電子署名 $D(TSSK_t, h(TI, VPK_n, TP_t))$ であり、従って、条項検証用署名ASGについて、発行者証明書 TP_t に含まれる発行者検証用公開鍵 $TSPK_t$ を用いて署名確認を行うことにより、チケット権利条項TI、有効性検証用公開鍵 VPK_n 、および発行者証明書 TP_t の改竄の有無を確認することができる。

【0146】

以上のように、電子チケットが、チケット有効性部とチケット権利条項部とから構成され、チケット有効性部は、電子チケットの有効性を表すものであるから、チケット有効性部の複製を防止すれば、電子チケットの複製を防止することができることになる。従って、チケット権利条項部は、複製されても問題はなく、チケット権利条項部を構成するチケット権利条項TIには、チケットとして必要十分な情報を含ませて、自由に公開することが可能になる。さらに、チケット有効性部は、それ自体を外部に示すことなく、その存在を証明することができるものであることから、外部への漏洩や複製を防止することができ、従って、不特定の第三者に対して、「権利証明」を行うことが可能となる。

【0147】

次に、図5は、図4の電子チケットを発行する図1のチケット発行装置3_tの構成例を示している。

【0148】

チケット条項取得部11は、電子チケットのチケット権利条項TI（図4）となる情報を取得し、チケット権利条項TIを生成して、条項検証用署名生成部16およびチケット生成部17に供給する。なお、チケット権利条項TIとなる情報としては、例えば、電子チケットがイベントのチケットであれば、日時、場所、イベント名、有効期限、通し番号などがある。但し、その情報の形式は自由である。

【0149】

ここで、電子チケットが反復使用できるものである場合、その有効期限や、使用回数の制限値は、チケット条項取得部11において、チケット権利条項TIとなる情報として取得される。また、チケット条項取得部11においては、例えば、図示せぬデータベースにあらかじめ登録された情報を取得するようにすることもできるし、チケット発行者が入力する情報を取得するようにすることもできる。

【0150】

発行者証明書取得部12は、図2で説明したようにして、チケット管理センタ1から発行される発行者証明書TP_tを、あらかじめ取得しており、条項検証用署名生成部16およびチケット生成部17に供給する。

【0151】

発行者署名生成用秘密鍵取得部 1 3 は、発行者署名生成用秘密鍵 $TSSK_t$ を取得し、条項検証用署名生成部 1 6 に供給する。なお、発行者署名生成用秘密鍵取得部 1 3 においては、例えば、図示せぬメモリに記憶された発行者署名生成用秘密鍵 $TSSK_t$ を取得するようにすることができる。

【 0 1 5 2 】

乱数発生部 1 4 は、有効性証明用秘密鍵 VSK_n と有効性検証用公開鍵 VPK_n を生成するための乱数を発生し、有効性鍵生成部 1 5 に供給する。

【 0 1 5 3 】

有効性鍵生成部 1 5 は、乱数発生部 1 4 からの乱数に基づいて、有効性証明用秘密鍵 VSK_n と有効性検証用公開鍵 VPK_n を生成し、チケット生成部 1 7 に供給する。また、有効性鍵生成部 1 5 は、有効性検証用公開鍵 VPK_n を、条項検証用署名生成部 1 6 にも供給する。なお、有効性鍵生成部 1 5 は、電子チケット # n ごとに、異なる有効性証明用秘密鍵 VSK_n と有効性検証用公開鍵 VPK_n を生成する。

【 0 1 5 4 】

条項検証用署名生成部 1 6 は、チケット条項取得部 1 1 からのチケット権利条項 TI 、発行者証明書取得部 1 2 からの発行者証明書 TP_t 、および有効性鍵生成部 1 5 からの有効性検証用公開鍵 VPK_n に対して、発行者署名生成用秘密鍵取得部 1 3 から供給される発行者署名生成用秘密鍵 $TSSK_t$ を用いて、条項検証用署名 ASG (図 4 (C)) となる電子署名を生成し、チケット生成部 1 7 に供給する。

【 0 1 5 5 】

チケット生成部 1 7 は、電子チケットの付加情報 (図 4 (B)) を生成し、その付加情報と、有効性鍵生成部 1 5 から供給される有効性証明用秘密鍵 VSK_n から、電子チケットのチケット有効性部を生成する。さらに、チケット生成部 1 7 は、チケット条項取得部 1 1 から供給されるチケット権利条項 TI 、発行者証明書取得部 1 2 から供給される発行者証明書 TP_t 、有効性鍵生成部 1 5 から供給される有効性検証用公開鍵 VPK_n 、および条項検証用署名生成部 1 6 から供給される条項検証用署名 ASG から、電子チケットのチケット権利条項部 (図 4 (C)) を生成する。そして、チケット生成部 1 7 は、チケット有効性部とチケット権利条項部から電子チケットを生成、発行し、チケット保持発行制御部 1 8 に供給する。

【 0 1 5 6 】

チケット保持発行制御部 1 8 は、基本的には、後述するチケット保持装置 4_uと同様の機能を有し、チケット生成部 1 7 からの電子チケットを保持し、チケット保持装置 4_uからの要求に応じて、電子チケットを、チケット保持装置 4_uに譲渡するために、電子チケットを外部に出力する。

【 0 1 5 7 】

なお、チケット発行装置 3_tにおける発行者署名生成用秘密鍵取得部 1 3、乱数発生部 1 4、有効性鍵生成部 1 5、条項検証用書署名生成部 1 6、チケット生成部 1 7、およびチケット保持発行制御部 1 8 は、耐タンパー性を有するように構成されている。

【 0 1 5 8 】

次に、図 6 のフローチャートを参照して、図 5 のチケット発行装置 3_tにおいて電子チケットを発行するチケット発行処理について説明する。

【 0 1 5 9 】

なお、発行者証明書取得部 1 2 においては、発行者証明書 TP_tが既に取得されており、条項検証用署名生成部 1 6 およびチケット生成部 1 7 に供給されているものとする。さらに、発行者署名生成用秘密鍵取得部 1 3 においても、発行者署名生成用秘密鍵 TSSK_tが既に取得されており、条項検証用署名生成部 1 6 に供給されているものとする。

【 0 1 6 0 】

チケット発行処理では、まず最初に、ステップ S 1 において、乱数発生部 1 4 が、乱数を発生し、有効性鍵生成部 1 5 に供給する。さらに、ステップ S 1 では、有効性鍵生成部 1 5 が、乱数発生部 1 4 からの乱数に基づいて、有効性証明用秘密鍵 VSK_nと有効性検証用公開鍵 VPK_nを生成し、チケット生成部 1 7 に供給して、ステップ S 2 に進む。

【 0 1 6 1 】

ステップ S 2 では、チケット生成部 1 7 が、電子チケットの付加情報を生成し、その付加情報と、有効性鍵生成部 1 5 から供給される有効性証明用秘密鍵 VSK_nから、電子チケットのチケット有効性部（図 4（B））を生成する。なお、電子

チケットの使用回数が制限されている場合には、付加情報には、電子チケットの使用回数が含まれるが、この使用回数は、付加情報の生成時に0回に初期化される。

【0162】

その後、ステップS3に進み、チケット条項取得部11が、電子チケットのチケット権利条項TIを生成し、条項検証用署名生成部16およびチケット生成部17に供給して、ステップS4に進む。ステップS4では、条項検証用署名生成部16が、チケット条項取得部11からのチケット権利条項TI、発行者証明書取得部12からの発行者証明書 TP_t 、および有効性鍵生成部15からの有効性検証用公開鍵 VPK_n に対して、発行者署名生成用秘密鍵取得部13から供給される発行者署名生成用秘密鍵 $TSSK_t$ を用いて、条項検証用署名ASG（図4（C））を生成し、チケット生成部17に供給して、ステップS5に進む。

【0163】

ステップS5では、チケット生成部17が、チケット条項取得部11から供給されるチケット権利条項TI、発行者証明書取得部12から供給される発行者証明書 TP_t 、有効性鍵生成部15から供給される有効性検証用公開鍵 VPK_n 、および条項検証用署名生成部16から供給される条項検証用署名ASGから、電子チケットのチケット権利条項部（図4（C））を生成し、ステップS6に進む。ステップS6では、チケット生成部17が、ステップS2で生成したチケット有効性部を、例えば、共通鍵暗号化方式により暗号化する。

【0164】

ここで、共通鍵暗号化方式は、対称暗号化方式とも呼ばれ、データを暗号化するのに用いられる鍵と、その暗号を復号するのに用いられる鍵が同一であるもの、あるいは、異なる場合でも一方の鍵から他方の鍵を算出することが容易であるもので、具体的なアルゴリズムとしては、例えば、DES(Data Encryption Standard)、Triple DES（アメリカ合衆国商務省標準局）、FEAL(Fast data Encipherment Algorithm)（日本電信電話株式会社）などがある。

【0165】

ステップS6においてチケット有効性部を暗号化した後は、ステップS7に進

み、チケット生成部 1 7 が、暗号化されたチケット有効性部とチケット権利条項部とを組にして電子チケットを生成し、チケット保持発行制御部 1 8 に供給する。チケット保持発行制御部 1 8 は、ステップ S 8 において、チケット生成部 1 7 からの電子チケットを保持し、チケット発行処理を終了する。

【0 1 6 6】

なお、チケット発行装置 3_t は、図 6 のチケット発行処理を繰り返し行うことで、複数の電子チケットを発行する。

【0 1 6 7】

以上のようにして、チケット保持発行制御部 1 8 に保持された電子チケットは、チケット保持発行制御部 1 8 において、後述するチケット譲渡処理が行われることにより、チケット保持装置 4_u (のユーザ) に譲渡される。

【0 1 6 8】

なお、電子チケットは、あらかじめ、チケット発行処理を行い、チケット保持発行制御部 1 8 に保持しておき、チケット保持装置 4_u から要求があった場合に、チケット保持発行制御部 1 8 からチケット保持装置 4_u に送信することによって譲渡することも可能であるし、チケット保持装置 4_u から要求されるごとに、チケット発行処理を行って譲渡することも可能である。

【0 1 6 9】

次に、図 7 は、図 1 のチケット保持装置 4_u の構成例を示している。

【0 1 7 0】

チケット保持装置 4_u は、自身が保持している電子チケットを、他のチケット保持装置 4_{u'} に譲渡する機能、チケット発行装置 3_t や他のチケット保持装置 4_{u'} が保持している電子チケットを譲受する機能、チケット検査装置 5_s に対して、自身が保持している電子チケットの一部であるチケット権利条項部を渡し、電子チケットに基づく権利の行使を行う機能、電子チケットを破棄する機能等を有する。

【0 1 7 1】

即ち、チケット授受制御部 2 1 は、自身が保持している電子チケットを譲渡する場合と、他のチケット保持装置 4_u から電子チケットを譲受する場合に、その

譲渡や譲受の制御を行う。さらに、チケット授受制御部 2 1 は、後述する処理を行うにあたり、各ブロックと通信しながら、必要な制御を行う。

【0 1 7 2】

装置証明書記憶部 2 2 は、図 3 で説明したようにして、チケット管理センタ 1 から、あらかじめ発行された装置証明書 AP_u を記憶しており、チケット授受制御部 2 1 の制御にしたがって、記憶している装置証明書 AP_u を、チケット授受制御部 2 1 に供給する。

【0 1 7 3】

乱数発生部 2 3 は、チケット授受制御部 2 1 または管理部 2 7 の制御にしたがって、乱数を発生し、チケット授受制御部 2 1 または管理部 2 7 に供給する。

【0 1 7 4】

署名処理部 2 4 は、チケット授受制御部 2 1 の制御にしたがい、必要に応じて、署名検証用公開鍵記憶部 2 5 に記憶された署名検証用公開鍵 P_{CA} 等を用いて、電子署名に関する処理を行う。

【0 1 7 5】

署名検証用公開鍵記憶部 2 5 は、チケット管理センタ 1 が公開している署名検証用公開鍵 P_{CA} をあらかじめ取得して記憶しており、その記憶している署名検証用公開鍵 P_{CA} を、必要に応じて、署名処理部 2 4 に供給する。

【0 1 7 6】

公開鍵暗号処理部 2 6 は、チケット管理センタ 1 に登録した装置検証用公開鍵 APK_u に対応する装置証明用秘密鍵 ASK_u を内蔵しており、チケット授受制御部 2 1 からの制御にしたがい、必要に応じて、装置証明用秘密鍵 ASK_u 等を用いて、公開鍵暗号化方式による暗号化処理と復号処理を行う。

【0 1 7 7】

管理部 2 7 は、チケット授受制御部 2 1 からの制御にしたがい、ストレージ部 2 8 に保持（記憶）された電子チケットの管理を行う。即ち、管理部 2 7 は、ストレージ部 2 8 に記憶された電子チケットの一部であるチケット有効性部を、その複製ができないように管理し、さらに、電子チケットを他のチケット保持装置（あるいは、チケット発行装置 3_t ）との間でやり取りする際に、そのやり取り

の途中で、電子チケットを、その複製ができないように移動し、また、ストレージ部 28 の電子チケットを譲渡した場合には、その譲渡した電子チケットを確実に削除する等の管理を行う。

【0178】

なお、管理部 27 は、親共通鍵記憶部 27A を内蔵しており、親共通鍵記憶部 27A は、共通鍵暗号化方式での暗号化と復号に用いられる共通鍵としての親共通鍵を記憶する。

【0179】

ストレージ部 28 は、管理部 27 によって管理され、電子チケットや、その電子チケットを管理するための管理情報を記憶する。なお、ストレージ部 28 は、外部から容易に着脱できないメモリや HD (Hard Disk) 等で構成することも可能であるし、外部から容易に着脱できるメモリカード等で構成することも可能である。

【0180】

共通鍵暗号処理部 29 は、管理部 27 からの制御にしたがい、共通鍵暗号化方式での暗号化と復号を行う。

【0181】

なお、チケット保持装置 4_u の装置証明書記憶部 22、乱数発生部 23、署名処理部 24、公開鍵暗号処理部 26、管理部 27、および共通鍵暗号処理部 29 は、耐タンパー性を有するように構成されている。

【0182】

次に、図 8 を参照して、図 7 の管理部 27 による、ストレージ部 28 に記憶された電子チケットの管理方法について説明する。

【0183】

なお、図 8 は、ストレージ部 28 に、J 個の電子チケット ETI_1 乃至 ETI_J が記憶されている状態を示している。また、図 8 において影を付してある部分は、暗号化されていることを表す。

【0184】

管理部 27 は、電子チケット ETI_j を、ストレージ部 28 に記憶させるが、電子

チケットETI_jを構成するチケット有効性部ETIA_jとチケット権利条項部ETIB_jのうち、チケット権利条項部ETIB_jについては、図8（A）に示すように、例えば、通常のコンピュータで扱われるファイルと同様にして、ストレージ部28に記憶させる。

【0185】

また、管理部27は、チケット有効性部ETIA_jについては、図8（A）に影を付して示すように、共通鍵暗号化方式により、電子チケットごとに異なる共通鍵で暗号化して、ストレージ部28に記憶させる。従って、チケット有効性部ETIA_jは、共通鍵暗号方式により、共通鍵で暗号化された形式のファイルとして、ストレージ部28に保存される。

【0186】

さらに、管理部27は、図8（B）に示すように、チケット有効性部ETIA_jを、共通鍵暗号化方式により暗号化および復号する共通鍵としての子共通鍵CK_jを、管理情報として、ストレージ部28に記憶させるが、その際、この管理情報としての子共通鍵CK_jを、管理部27が内蔵する親共通鍵記憶部27Aに記憶された親共通鍵PKで共通鍵暗号化方式により暗号化する。このように、チケット有効性部ETIA_jの暗号化に用いられた子共通鍵CK_jも、親共通鍵PKで暗号化された形で、ストレージ部28に記憶される。

【0187】

なお、電子チケットETI_jを構成するチケット有効性部ETIA_jとチケット権利条項部ETIB_jとの対応関係、並びにチケット有効性部ETIA_jと、その暗号化および復号に用いられる子共通鍵CK_jとの対応関係は、管理情報に含められるか、あるいは、独立のファイルとして、ストレージ部28に保存される。

【0188】

また、親共通鍵PKと、管理情報としての子共通鍵CK_jは、所定のタイミングで更新される。即ち、親共通鍵PKは、例えば、管理情報を構成する子共通鍵CK_jが変更されるごとに更新される。また、子共通鍵CK_jは、例えば、ストレージ部28に記憶される電子チケットが変更されるごとに更新される。なお、更新のための新たな親共通鍵PKと子共通鍵CK_jは、例えば、後述するように、乱数に基づい

て生成される。

【0189】

以上のように、ストレージ部28では、チケット有効性部ETIA_jが、子共通鍵CK_jで暗号化されて記憶され、さらに、その子共通鍵CK_jも親共通鍵PKで暗号化されて記憶されているので、チケット保持装置4_uに保持（記憶）されているチケット有効性部ETIA_jの漏洩を強固に防止することができる。

【0190】

次に、図9のフローチャートを参照して、図7のチケット保持装置4_uにおいて、チケット発行装置3_tまたは他のチケット保持装置4_{u'}から電子チケットを譲受する場合に行われるチケット譲受処理について説明する。

【0191】

なお、以下においては、他のチケット保持装置4_{u'}から電子チケットを譲受するものとして、チケット保持装置4_uによるチケット譲受処理の説明を行うが、チケット発行装置3_tから電子チケットを譲受する場合にも、チケット保持装置4_uでは、同様の処理が行われる。

【0192】

チケット譲受処理では、まず最初に、ステップS11において、後述する譲受側の認証処理が行われ、ステップS12に進む。ステップS12では、チケット授受制御部21が、ステップS11における認証が成功したかどうかを判定し、成功しなかった（失敗した）と判定した場合、以降の処理をスキップして、チケット譲受処理を終了する。即ち、認証が失敗した場合には、電子チケットの譲渡を行おうとしている相手の装置である他のチケット保持装置4_{u'}（またはチケット発行装置3_t）が正当なものではないとして、チケット保持装置4_uは、そのような正当でない装置からの電子チケットの譲受を拒否する。

【0193】

一方、ステップS12において、認証が成功したと判定された場合、即ち、電子チケットの譲渡を行おうとしている相手の装置である他のチケット保持装置4_{u'}が正当なものである場合、ステップS13に進み、後述するように、正当な他のチケット保持装置4_{u'}は、譲渡しようとしている電子チケットのチケット

権利条項部を送信してくるので、チケット授受制御部21は、そのチケット権利条項部を受信する。

【0194】

そして、ステップS14に進み、チケット授受制御部21は、ステップS13で受信したチケット権利条項部の正当性を確認する、後述するチケット権利条項部の確認処理を行い、ステップS15に進む。ステップS15では、チケット授受制御部21は、ステップS13で受信したチケット権利条項部の正当性が確認されたかどうかを判定し、正当性を確認することができなかったと判定した場合、以降の処理をスキップして、チケット譲受処理を終了する。即ち、チケット権利条項部の正当性を確認することができなかった場合には、チケット権利条項部が改竄されているとして、チケット保持装置4_uは、そのような改竄が行われているチケット権利条項部を有する電子チケットの譲受を拒否する。

【0195】

一方、ステップS15において、チケット権利条項部の正当性を確認することができたと判定された場合、ステップS16に進み、後述するように、他のチケット保持装置4_uは、自身の装置証明書AP_uを送信してくるので、チケット授受制御部21は、その装置証明書AP_uを受信する。

【0196】

そして、ステップS17に進み、チケット授受制御部21は、ステップS16で受信した他のチケット保持装置4_uの装置証明書AP_u（図3）を確認する。

【0197】

即ち、チケット授受制御部21は、装置証明書AP_uを、署名処理部24に供給し、その装置証明書AP_uに含まれる電子署名ASG_uの署名確認を行わせる。

【0198】

この場合、署名処理部24は、装置証明書AP_uに含まれる電子署名ASG_uを、署名検証用公開鍵記憶部25に記憶されたチケット管理センタ1の署名検証用公開鍵P_{CA}で暗号化処理し、その暗号化結果と、装置証明書AP_uに含まれる他のチケット保持装置4_uの装置検証用公開鍵APK_uとの一致性を判定する。そして、署名処理部24は、その一致性の判定結果を、チケット授受制御部21に

供給する。

【0199】

チケット授受制御部21は、署名処理部24から一致性の判定結果を受信すると、ステップS18に進み、その一致性の判定結果に基づき、装置証明書 AP_u が正当なものであるかどうかを判定する。ステップS18において、装置証明書 AP_u が正当なものでないと判定された場合、即ち、装置証明書 AP_u に含まれる電子署名 ASG_u の、署名検証用公開鍵 P_{CA} による暗号化結果と、その装置証明書 AP_u に含まれる装置検証用公開鍵 APK_u との一致性が認められない場合、以降の処理をスキップして、チケット譲受処理を終了する。即ち、この場合、電子署名 ASG_u または装置検証用公開鍵 APK_u が改竄されているとして、チケット保持装置4_uは、そのような改竄が行われている装置証明書 AP_u を有する他のチケット保持装置4_uからの電子チケットの譲受を拒否する。

【0200】

一方、ステップS18において、装置証明書 AP_u が正当なものであると判定された場合、即ち、装置証明書 AP_u に含まれる電子署名 ASG_u の、署名検証用公開鍵 P_{CA} による暗号化結果と、その装置証明書 AP_u に含まれる装置検証用公開鍵 APK_u との一致性が認められた場合、ステップS19に進み、チケット授受制御部21は、乱数発生部23を制御することにより、乱数を発生させ、その乱数から、共通鍵暗号化方式の暗号化および復号に用いる共通鍵としての暗号鍵UKを生成する。

【0201】

そして、ステップS20に進み、チケット授受制御部21は、その暗号鍵UKと、正当性が確認された装置証明書 AP_u に含まれる装置検証用公開鍵 APK_u を、公開鍵暗号処理部26に供給し、公開鍵暗号処理部26を制御することにより、暗号鍵UKを、装置検証用公開鍵 APK_u で暗号化した暗号化暗号鍵 $E(APK_u, UK)$ を生成させて、ステップS21に進む。

【0202】

ステップS21では、チケット授受制御部21は、暗号化暗号鍵 $E(APK_u, UK)$ を、電子チケットを譲渡しようとしている他のチケット保持装置4_uに送信し

、ステップS 2 2に進む。ステップS 2 2では、後述するように、暗号化暗号鍵 $E(APK_u, UK)$ を受信した他のチケット保持装置 4_u が、譲渡しようとしている電子チケットのチケット有効性部を暗号鍵UKで暗号化した暗号化チケット有効性部を送信してくるので、チケット授受制御部2 1は、その暗号化チケット有効性部を受信する。

【0 2 0 3】

そして、ステップS 2 3に進み、チケット授受制御部2 1は、ステップS 2 2で暗号化チケット有効性部を正常受信することができたかどうかを判定し、できなかったと判定した場合、ステップS 2 4をスキップして、チケット譲受処理を終了する。この場合、電子チケットの譲受は失敗となる。

【0 2 0 4】

また、ステップS 2 3において、暗号化チケット有効性部を正常受信することができたと判定された場合、ステップS 2 4に進み、ストレージ部2 8に、電子チケットを追加記憶させる、後述するチケット追加処理が行われ、これにより、電子チケットの譲受に成功して、チケット授受処理を終了する。

【0 2 0 5】

次に、図1 0のフローチャートを参照して、図9のステップS 1 1における譲受側の認証処理について詳述する。

【0 2 0 6】

譲受側の認証処理では、まず最初に、ステップS 3 1において、チケット授受制御部2 1は、装置証明書記憶部2 2に記憶された装置証明書 AP_u を読み出し、電子チケットを譲渡しようとしている他のチケット保持装置 4_u に送信して、ステップS 3 2に進む。

【0 2 0 7】

ステップS 3 2では、後述するように、装置証明書 AP_u を受信した他のチケット保持装置 4_u が、その装置証明書 AP_u に含まれる装置検証用公開鍵 APK_u で乱数 r を暗号化した暗号化乱数 $R=E(APK_u, r)$ を送信してくるので、チケット授受制御部2 1は、その暗号化乱数 R を受信する。

【0 2 0 8】

そして、ステップ S 3 3 に進み、チケット授受制御部 2 1 は、暗号化乱数 R を、公開鍵暗号処理部 2 6 に供給し、その内蔵する装置証明用秘密鍵 ASK_u で復号させ、ステップ S 3 4 に進む。

【 0 2 0 9 】

ステップ S 3 4 では、チケット授受制御部 2 1 は、装置証明用秘密鍵 ASK_u による暗号化乱数 R の復号結果 $r' = D(ASK_u, R)$ を、他のチケット保持装置 4_u に送信し、ステップ S 3 5 に進む。

【 0 2 1 0 】

ステップ S 3 5 では、後述するように、暗号化乱数 R の復号結果 r' を受信した他のチケット保持装置 4_u が、その復号結果 r' に基づいて、認証を行い、その認証結果を表す認証メッセージが送信されてくるので、チケット授受制御部 2 1 は、その認証メッセージを受信し、その認証メッセージに基づいて、他のチケット保持装置 4_u における認証が成功したかどうかを判定する。

【 0 2 1 1 】

ステップ S 3 5 において、認証が成功したと判定された場合、ステップ S 3 6 に進み、チケット授受制御部 2 1 は、認証が成功したことを認識し、譲受側の認証処理を終了する。また、ステップ S 3 5 において、認証が成功しなかったと判定された場合、ステップ S 3 7 に進み、チケット授受制御部 2 1 は、認証が失敗したことを認識して、譲受側の認証処理を終了する。

【 0 2 1 2 】

なお、ステップ S 3 6 または S 3 7 の認識結果に基づき、図 9 におけるステップ S 1 2 の判定処理が行われることになる。

【 0 2 1 3 】

次に、図 1 1 のフローチャートを参照して、図 9 のステップ S 1 4 におけるチケット権利条項部の確認処理について詳述する。

【 0 2 1 4 】

チケット権利条項部の確認処理では、まず最初に、ステップ S 4 1 において、チケット授受制御部 2 1 は、電子チケットを譲渡しようとしている他のチケット保持装置 4_u から、図 9 のステップ S 1 3 において受信したチケット権利条項

部に含まれる発行者証明書 TP_t (図4 (C)) を抽出し、ステップS42に進む。ステップS42では、チケット授受制御部21は、ステップS41で抽出した発行者証明書 TP_t を確認する。

【0215】

即ち、チケット授受制御部21は、発行者証明書 TP_t を、署名処理部24に供給し、その発行者証明書 TP_t に含まれる電子署名 TSG_t の署名確認を行わせる。

【0216】

この場合、署名処理部24は、発行者証明書 TP_t に含まれる電子署名 TSG_t を、署名検証用公開鍵記憶部25に記憶されたチケット管理センタ1の署名検証用公開鍵 P_{CA} で暗号化処理し、その暗号化結果と、発行者証明書 TP_t に含まれる識別情報 TID_t および発行者検証用公開鍵 $TSPK_t$ の組との一致性を判定する。そして、署名処理部24は、その一致性の判定結果を、チケット授受制御部21に供給する。

【0217】

チケット授受制御部21は、署名処理部24から一致性の判定結果を受信すると、ステップS43に進み、その一致性の判定結果に基づき、発行者証明書 TP_t が正当なものであるかどうかを判定する。ステップS43において、発行者証明書 TP_t が正当なものでないと判定された場合、即ち、発行者証明書 TP_t に含まれる電子署名 TSG_t の、署名検証用公開鍵 P_{CA} による暗号化結果と、その発行者証明書 TP_t に含まれる識別情報 TID_t および発行者検証用公開鍵 $TSPK_t$ の組との一致性が認められない場合、ステップS48に進み、チケット授受制御部21は、発行者証明書 TP_t が改竄等されており、正当なものであることを確認することができなかったことを認識し、即ち、発行者証明書 TP_t の正当性の確認に失敗したことを認識し、チケット権利条項部の確認処理を終了する。

【0218】

一方、ステップS43において、発行者証明書 TP_t が正当なものであると判定された場合、即ち、発行者証明書 TP_t に含まれる電子署名 TSG_t の、署名検証用公開鍵 P_{CA} による暗号化結果と、その発行者証明書 TP_t に含まれる識別情報 TID_t および発行者検証用公開鍵 $TSPK_t$ の組との一致性が認められた場合、ステップS4

4に進み、チケット授受制御部21は、図9のステップS13において受信したチケット権利条項部（図4（C））に含まれる条項検証用署名ASGと、チケット権利条項TI、有効性検証用公開鍵VPK_n、および発行者証明書TP_tの組とを抽出するとともに、その発行者証明書TP_tに含まれる発行者検証用公開鍵TSPK_tを抽出し、ステップS45に進む。ステップS45では、チケット授受制御部21は、ステップS44で抽出した条項検証用署名ASGの署名確認を行う。

【0219】

即ち、チケット授受制御部21は、ステップS44で抽出した条項検証用署名ASGと、チケット権利条項TI、有効性検証用公開鍵VPK_n、および発行者証明書TP_tの組と、発行者検証用公開鍵TSPK_tとを、署名処理部24に供給し、条項検証用署名ASGの署名確認を行わせる。

【0220】

この場合、署名処理部24は、条項検証用署名ASGを、発行者検証用公開鍵TSPK_tで暗号化処理し、その暗号化結果と、チケット権利条項TI、有効性検証用公開鍵VPK_n、および発行者証明書TP_tの組との一致性を判定する。そして、署名処理部24は、その一致性の判定結果を、チケット授受制御部21に供給する。

【0221】

チケット授受制御部21は、署名処理部24から一致性の判定結果を受信すると、ステップS46に進み、その一致性の判定結果に基づき、図9のステップS13において受信したチケット権利条項部が正当なものかどうかを判定する。ステップS46において、チケット権利条項部が正当なものでないと判定された場合、即ち、条項検証用署名ASGの、発行者検証用公開鍵TSPK_tによる暗号化結果と、チケット権利条項TI、有効性検証用公開鍵VPK_n、および発行者証明書TP_tの組との一致性が認められない場合、ステップS48に進み、チケット授受制御部21は、チケット権利条項部が改竄等されており、正当なものであることを確認することができなかったことを認識し、即ち、チケット権利条項部の正当性の確認に失敗したことを認識し、チケット権利条項部の確認処理を終了する。

【0222】

一方、ステップS46において、チケット権利条項部が正当なものであると判

定された場合、即ち、条項検証用署名ASGの、発行者検証用公開鍵TSPK_tによる暗号化結果と、チケット権利条項TI、有効性検証用公開鍵VPK_n、および発行者証明書TP_tの組との一致性が認められる場合、ステップS 4 7に進み、チケット授受制御部 2 1は、チケット権利条項部が改竄等されていない、正当なものであることを確認することができたことを認識し、即ち、チケット権利条項部の正当性の確認に成功したことを認識し、チケット権利条項部の確認処理を終了する。

【 0 2 2 3 】

なお、ステップS 4 7またはS 4 8の認識結果に基づき、図9におけるステップS 1 5の判定処理が行われることになる。

【 0 2 2 4 】

次に、図12のフローチャートを参照して、図9のステップS 2 4におけるチケット追加処理について詳述する。

【 0 2 2 5 】

チケット追加処理では、まず最初に、ステップS 5 1において、チケット授受制御部 2 1は、管理部 2 7を制御することにより、他のチケット保持装置4_uから、図9のステップS 1 3で受信したチケット権利条項部と、ステップS 2 2で受信した暗号化チケット有効性部とを、ストレージ部 2 8に追加記憶させ、ステップS 5 2に進む。

【 0 2 2 6 】

ステップS 5 2では、管理部 2 7が、ストレージ部 2 8に記憶されている、暗号化された管理情報としての子共通鍵CK_jを読み出すとともに、親共通鍵記憶部 2 7 Aに記憶されている親共通鍵PKを読み出し、共通鍵記憶部 2 9に供給して、暗号化されている子共通鍵CK_jを、親共通鍵PKで復号させる。

【 0 2 2 7 】

そして、ステップS 5 3に進み、管理部 2 7は、図9のステップS 1 9で生成された暗号鍵UKを、チケット授受制御部 2 1から取得し、その暗号鍵UKを、ステップS 5 2でストレージ部 2 8から読み出した管理情報に、新たな子共通鍵として追加して、ステップS 5 4に進む。

【 0 2 2 8 】

ステップS54では、管理部27は、乱数発生部23に乱数を発生させ、その乱数から、新たな親共通鍵PKを生成して、親共通鍵記憶部27の記憶内容を、その新たな親共通鍵PKで更新する（親共通鍵記憶部27に、新たな親共通鍵PKを上書きする）。

【0229】

そして、ステップS55に進み、管理部27は、新たな親共通鍵PKと、暗号鍵UKを新たな子共通鍵として追加した管理情報（以下、適宜、新たな管理情報という）とを、共通鍵暗号処理部29に供給し、新たな管理情報を、新たな親共通鍵PKで暗号化させる。さらに、管理部27は、ステップS55において、その暗号化された新たな管理情報を、ストレージ部28に上書きする形で記憶させ、チケット追加処理を終了する。

【0230】

なお、ステップS51においてストレージ部28に記憶される暗号化チケット有効性部は、後述するように、電子チケットを譲渡した他のチケット保持装置4_{u'}において、新たな子共通鍵として管理情報に追加される暗号鍵UKで、チケット有効性部が暗号化されたものであり、電子チケットを譲受するチケット保持装置4_uでは、ストレージ部28に記憶させる前に、特に処理する必要はない。

【0231】

次に、図13のフローチャートを参照して、図5のチケット発行装置3_tまたは図7のチケット保持装置4_uにおいて、他のチケット保持装置4_{u'}に電子チケットを譲渡する場合に行われるチケット譲渡処理について説明する。

【0232】

なお、以下においては、チケット保持装置4_uから電子チケットを譲渡するものとして、チケット譲渡処理の説明を行うが、チケット発行装置3_tから電子チケットを譲渡する場合にも、チケット発行装置3_tのチケット保持発行制御部18において、同様の処理が行われる。

【0233】

ここで、チケット譲渡処理には、図3で説明した装置証明用秘密鍵ASK_u、装置検証用公開鍵APK_u、およびチケット管理センタ1が発行する装置証明書AP_uが必

要であり、従って、チケット発行装置 3_t のチケット保持発行制御部 18 がチケット譲渡処理を行うには、これらの装置証明用秘密鍵 ASK_t 、装置検証用公開鍵 APK_t 、および装置証明書 AP_t を有している必要がある。

【 0 2 3 4 】

チケット譲渡処理では、まず最初に、ステップ S 6 1 において、後述する譲渡側の認証処理が行われ、ステップ S 6 2 に進む。ステップ S 6 2 では、チケット授受制御部 21 が、ステップ S 6 1 における認証が成功したかどうかを判定し、成功しなかった（失敗した）と判定した場合、以降の処理をスキップして、チケット譲渡処理を終了する。即ち、認証が失敗した場合には、電子チケットの譲渡相手の装置である他のチケット保持装置 4_u が正当なものではないとして、チケット保持装置 4_u は、そのような正当でない装置への電子チケットの譲渡を拒否する。

【 0 2 3 5 】

一方、ステップ S 6 2 において、認証が成功したと判定された場合、即ち、電子チケットの譲渡相手の装置である他のチケット保持装置 4_u が正当なものである場合、ステップ S 6 3 に進み、チケット授受制御部 21 は、管理部 27 を制御することにより、ストレージ部 28 から、譲渡しようとしている電子チケットのチケット条項部を読み出させ、譲渡相手である他のチケット保持装置 4_u に送信して、ステップ S 6 4 に進む。

【 0 2 3 6 】

ステップ S 6 4 では、チケット授受制御部 21 は、装置証明書記憶部 22 に記憶された装置証明書 AP_u を読み出し、譲渡相手である他のチケット保持装置 4_u に送信する。

【 0 2 3 7 】

譲渡相手である他のチケット保持装置 4_u では、上述のチケット譲受処理（図 9）が行われ、ステップ S 6 3 で送信したチケット権利条項部と、ステップ S 6 4 で送信した装置証明書 AP_u の正当性が確認されると、チケット譲受処理のステップ S 2 1 で、暗号化暗号鍵 $E(APK_u, UK)$ を送信してくるので、チケット授受制御部 21 は、ステップ S 6 5 において、その暗号化暗号鍵 $E(APK_u, UK)$ を受信する

【 0 2 3 8 】

そして、ステップ S 6 6 に進み、チケット授受制御部 2 1 は、ステップ S 6 5 で受信した暗号化暗号鍵 $E(APK_u, UK)$ を復号する。

【 0 2 3 9 】

即ち、暗号化暗号鍵 $E(APK_u, UK)$ は、ステップ S 6 4 において、譲渡相手である他のチケット保持装置 4_u に対して送信した装置証明書 AP_u に含まれる装置検証用公開鍵 APK_u を用いて、譲渡相手である他のチケット保持装置 4_u が、暗号鍵 UK を暗号化したものであり、従って、公開鍵暗号処理部 2 6 が内蔵する装置証明用秘密鍵 ASK_u で復号することができる。

【 0 2 4 0 】

そこで、ステップ S 6 6 では、チケット授受制御部 2 1 は、暗号化暗号鍵 $E(APK_u, UK)$ を、公開鍵暗号処理部 2 6 に供給し、装置証明用秘密鍵 ASK_u を用いて、暗号鍵 UK に復号させる。

【 0 2 4 1 】

チケット授受制御部 2 1 は、以上のようにして、暗号鍵 UK を得た後、ステップ S 6 6 からステップ S 6 7 に進み、管理部 2 7 を制御することにより、ストレージ部 2 8 に記憶された、譲渡しようとしてる電子チケットの暗号化チケット有効性部を復号させる。

【 0 2 4 2 】

即ち、この場合、管理部 2 7 は、親共通鍵記憶部 2 7 A に記憶された親共通鍵 PK を読み出すとともに、ストレージ部 2 8 に記憶された暗号化された管理情報（以下、適宜、暗号化管理情報という）を読み出し、共通鍵暗号処理部 2 9 に供給する。共通鍵暗号処理部 2 9 は、暗号化管理情報を、親共通鍵 PK を用いて、管理情報に復号し、その管理情報から、譲渡しようとしてる電子チケットのチケット有効性部の暗号化に用いた子共通鍵 CK_j を抽出する。

【 0 2 4 3 】

その後、管理部 2 7 は、ストレージ部 2 8 から、譲渡しようとしてる電子チケットの暗号化チケット有効性部を読み出し、共通鍵暗号処理部 2 9 に供給する。

共通鍵暗号処理部 29 は、暗号化チケット有効性部を、管理情報から抽出した子共通鍵 CK_i を用いて、チケット有効性部に復号する。

【0244】

共通鍵暗号処理部 29 において、以上のようにして、チケット有効性部が復号されると、ステップ S68 に進み、チケット授受制御部 21 は、ステップ S66 で復号した暗号鍵 UK を、管理部 27 に供給し、その暗号鍵 UK によるチケット有効性部の暗号化を要求する。この場合、管理部 27 は、暗号鍵 UK を、共通鍵暗号処理部 29 に供給し、その暗号鍵 UK を用いて、ステップ S67 で復号したチケット有効性部を暗号化させる。

【0245】

共通鍵暗号処理部 29 において、暗号鍵 UK によるチケット有効性部の暗号化が行われることにより得られる暗号化チケット有効性部は、管理部 27 を介して、チケット授受制御部 21 に供給される。チケット授受制御部 21 は、ステップ S69 において、その暗号化チケット有効性部を、譲渡相手である他のチケット保持装置 4_u に対して送信し、ステップ S70 に進む。

【0246】

ステップ S70 では、ストレージ部 28 から、譲渡した電子チケットを削除する、後述するチケット削除処理が行われ、チケット譲渡処理を終了する。

【0247】

次に、図 14 のフローチャートを参照して、図 13 のステップ S61 における譲渡側の認証処理について詳述する。

【0248】

譲渡側の認証処理では、まず最初に、ステップ S81 において、チケット授受制御部 21 は、譲渡相手である（電子チケットを譲受する）他のチケット保持装置 4_u が、譲受側の認証処理（図 10）のステップ S31 で送信してくる装置証明書 AP_u （図 3）を受信し、ステップ S82 に進む。

【0249】

ステップ S82 では、チケット授受制御部 21 は、ステップ S81 で受信した他のチケット保持装置 4_u の装置証明書 AP_u を確認する。

【 0 2 5 0 】

即ち、チケット授受制御部 2 1 は、装置証明書 AP_u を、署名処理部 2 4 に供給し、その装置証明書 AP_u に含まれる電子署名 ASG_u の署名確認を行わせる。

【 0 2 5 1 】

この場合、署名処理部 2 4 は、装置証明書 AP_u に含まれる電子署名 ASG_u を、署名検証用公開鍵記憶部 2 5 に記憶されたチケット管理センタ 1 の署名検証用公開鍵 P_{CA} で暗号化処理し、その暗号化結果と、装置証明書 AP_u に含まれる他のチケット保持装置 4_u の装置検証用公開鍵 APK_u との一致性を判定する。そして、署名処理部 2 4 は、その一致性の判定結果を、チケット授受制御部 2 1 に供給する。

【 0 2 5 2 】

チケット授受制御部 2 1 は、署名処理部 2 4 から一致性の判定結果を受信すると、ステップ S 8 3 に進み、その一致性の判定結果に基づき、装置証明書 AP_u が正当なものであるかどうかを判定する。ステップ S 8 3 において、装置証明書 AP_u が正当なものでないと判定された場合、即ち、装置証明書 AP_u に含まれる電子署名 ASG_u の、署名検証用公開鍵 P_{CA} による暗号化結果と、その装置証明書 AP_u に含まれる装置検証用公開鍵 APK_u との一致性が認められない場合、ステップ S 9 0 に進み、認証が失敗したことを認識するとともに、その旨の認証メッセージを、譲渡相手の他のチケット保持装置 4_u に送信して、譲渡側の認証処理を終了する。

【 0 2 5 3 】

一方、ステップ S 8 3 において、装置証明書 AP_u が正当なものであると判定された場合、即ち、装置証明書 AP_u に含まれる電子署名 ASG_u の、署名検証用公開鍵 P_{CA} による暗号化結果と、その装置証明書 AP_u に含まれる装置検証用公開鍵 APK_u との一致性が認められた場合、ステップ S 8 4 に進み、チケット授受制御部 2 1 は、乱数発生部 2 3 を制御することにより、乱数 r を発生させ、ステップ S 8 5 に進む。

【 0 2 5 4 】

ステップ S 8 5 では、チケット授受制御部 2 1 は、正当なものであることが確

認された装置証明書 $AP_{u'}$ に含まれる装置検証用公開鍵 $APK_{u'}$ を抽出し、乱数 r とともに、公開鍵暗号処理部26に供給することで、乱数 r を、装置検証用公開鍵 $APK_{u'}$ で暗号化させる。

【0255】

そして、ステップS86に進み、チケット授受制御部21は、公開鍵暗号処理部26において、装置検証用公開鍵 $APK_{u'}$ による乱数 r の暗号化が行われることにより得られた暗号化乱数 $R=E(APK_{u'}, r)$ を、譲渡相手の他のチケット保持装置 $4_{u'}$ に送信し、ステップS87に進む。

【0256】

暗号化乱数 $R=E(APK_{u'}, r)$ を受信した他のチケット保持装置 $4_{u'}$ では、上述の譲受側の認証処理(図10)のステップS33において、暗号化乱数 $R=E(APK_{u'}, r)$ を、装置証明用秘密鍵 $ASK_{u'}$ で復号し、さらに、ステップS34において、その暗号化乱数 R の復号結果 $r'=D(ASK_{u'}, R)$ を送信してくるので、ステップS87では、チケット授受制御部21が、その復号結果 $r'=D(ASK_{u'}, R)$ を受信し、ステップS88に進む。

【0257】

ステップS88では、チケット授受制御部21は、ステップS84で発生した乱数 r と、ステップS87で受信した暗号化乱数 R の復号結果 r' とが一致するかどうかを判定する。ステップS88において、乱数 r と、暗号化乱数 R の復号結果 r' とが一致しないと判定された場合、ステップS90に進み、チケット授受制御部21は、譲渡相手の他のチケット保持装置 $4_{u'}$ が、チケット管理センタ1に登録されていない装置(正当でない装置)であるとして、認証が失敗したことを認識し、さらに、その旨の認証メッセージを、譲渡相手の他のチケット保持装置 $4_{u'}$ に送信して、譲渡側の認証処理を終了する。

【0258】

一方、ステップS88において、乱数 r と、暗号化乱数 R の復号結果 r' とが一致すると判定された場合、ステップS89に進み、チケット授受制御部21は、譲渡相手の他のチケット保持装置 $4_{u'}$ が、チケット管理センタ1に登録されている正当な装置であるとして、認証が成功したことを認識し、さらに、その旨の

認証メッセージを、譲渡相手の他のチケット保持装置 4_u に送信して、譲渡側の認証処理を終了する。

【0259】

なお、ステップ S 8 9 または S 9 0 の認識結果に基づき、図 1 3 におけるステップ S 6 2 の判定処理が行われることになる。

【0260】

次に、図 1 5 のフローチャートを参照して、図 1 3 のステップ S 7 0 におけるチケット削除処理について詳述する。

【0261】

チケット削除処理では、まず最初に、ステップ S 1 0 1 において、管理部 2 7 は、ストレージ部 2 8 に記憶されている暗号化管理情報を読み出すとともに、親共通鍵記憶部 2 7 A に記憶されている親共通鍵 PK を読み出し、共通鍵記憶部 2 9 に供給して、暗号化管理情報を、親共通鍵 PK を用いて、管理情報に復号させる。

【0262】

そして、ステップ S 1 0 2 に進み、管理部 2 7 は、削除対象の電子チケットのチケット有効性部の暗号化に用いた子共通鍵 CK_j を、ステップ S 1 0 1 で復号された管理情報から削除し、ステップ S 1 0 3 に進む。

【0263】

ここで、削除対象の電子チケットとは、電子チケットの譲渡が行われた場合には、その譲渡された電子チケットを意味する。

【0264】

ステップ S 1 0 3 では、管理部 2 7 は、乱数発生部 2 3 に乱数を発生させ、その乱数から、新たな親共通鍵 PK を生成して、親共通鍵記憶部 2 7 の記憶内容を、その新たな親共通鍵 PK で更新する（親共通鍵記憶部 2 7 に、新たな親共通鍵 PK を上書きする）。

【0265】

そして、ステップ S 1 0 4 に進み、管理部 2 7 は、ステップ S 1 0 2 で、削除対象の電子チケットのチケット有効性部の暗号化に用いた子共通鍵 CK_j を削除した管理情報と、ステップ S 1 0 3 で得られた新たな親共通鍵 PK を、共通鍵暗号処

理部 2 9 に供給し、その管理情報を、新たな親共通鍵 PK で暗号化させることにより、新たな暗号化管理情報を得る。さらに、ステップ S 1 0 4 において、管理部 2 7 は、その新たな暗号化管理情報を、ストレージ部 2 8 に上書きする形で記憶させ、ステップ S 1 0 5 に進む。

【 0 2 6 6 】

ステップ S 1 0 5 では、管理部 2 7 は、ストレージ部 2 8 から、削除対象の電子チケットを構成する暗号化チケット有効性部とチケット権利条項部を削除し、チケット削除処理を終了する。

【 0 2 6 7 】

なお、図 1 5 のチケット削除処理は、電子チケットが譲渡された場合に、その電子チケットを削除対象として行われる他、電子チケットのチケット権利条項部の記述、あるいは暗黙の仮定によって、電子チケットの有効期間や、使用回数の制限値を越えた場合、さらには、所有者の意志により、不要となった電子チケットが存在する場合等に、その電子チケットを削除対象として行われる。

【 0 2 6 8 】

次に、図 1 6 のフローチャートを参照して、図 7 のチケット保持装置 4_uにおいて、チケット検査装置 5_sに対して、電子チケットに基づく権利を行使または証明する場合に行われるチケットの権利行使／証明処理について説明する。

【 0 2 6 9 】

なお、説明の便宜上、使用回数が制限された電子チケットに基づく権利を行使する際に、使用回数も含めて、電子チケットの権利を証明し、その結果として、使用回数が 1 回増加する場合を、以下、適宜、権利行使という。また、電子チケットの有効性だけを示す場合、および使用回数の制限のない電子チケット（有効期限や日付の指定は、あってもかまわない）に基づく権利を行使する場合のように、電子チケットを所有していることを示す場合を、以下、適宜、権利証明という。

【 0 2 7 0 】

従って、例えば、電子チケットが回数券で、その回数券によって、改札を通る場合等が、権利行使に該当する。また、電子チケットが定期券で、その定期券に

よって、改札を通る場合や、新幹線の車内において、乗車券や特急券としての電子チケットを見せる場合等が、権利証明に該当する。なお、電子チケットの譲渡が行われる場合に、受け取ろうとしている電子チケットや、受け取った電子チケットの有効性の確認を行うことも、権利証明に該当する。

【0271】

チケットの権利行使／証明処理では、まず最初に、例えば、ユーザが、チケット保持装置4_uのストレージ部28に保持（記憶）されている電子チケットのうち、権利を行使または証明しようとしている電子チケットを選択する。ここで、このようにして選択された電子チケットを、以下、適宜、注目電子チケットという。

【0272】

そして、ステップS111において、チケット授受制御部21は、管理部27を制御することにより、注目電子チケットのチケット権利条項部を、ストレージ部28から読み出させる。さらに、ステップS111では、チケット授受制御部21は、ストレージ部28から読み出されたチケット権利条項部を、チケット検査装置5_sに送信し、ステップS112に進む。

【0273】

ステップS112では、後述するように、チケット保持装置4_uからチケット権利条項部を受信したチケット検査装置5_sが、乱数rを送信してくるので、チケット授受制御部21は、その乱数rを受信し、ステップS113に進む。

【0274】

ステップS113では、管理部27は、ストレージ部28に記憶されている暗号化管理情報を読み出すとともに、親共通鍵記憶部27Aに記憶されている親共通鍵PKを読み出し、共通鍵記憶部29に供給して、暗号化管理情報を、親共通鍵PKを用いて、管理情報に復号させる。

【0275】

そして、ステップS114に進み、管理部27は、復号された管理情報から、注目電子チケットのチケット有効性部の暗号化に用いた子共通鍵CK_jを抽出し、ステップS115に進む。ステップS115では、管理部27は、ストレージ部

28から、注目電子チケットの暗号化チケット有効性部を読み出し、ステップS114で得た子共通鍵 CK_j とともに、共通鍵暗号処理部29に供給して、暗号化チケット有効性部を復号させる。

【0276】

即ち、この場合、共通鍵暗号処理部29は、暗号化チケット有効性部を、子共通鍵 CK_j で、チケット有効性部に復号し、管理部27を介して、チケット授受制御部21に供給する。

【0277】

その後、チケット授受制御部21は、ステップS116に進み、ステップS11でチケット検査装置5_sに送信した注目電子チケットのチケット権利条項部（図4（C））におけるチケット権利条項TIを参照することにより、注目電子チケットに基づく権利が、使用回数の制限されているもの（以下、適宜、回数制限付きの権利という）であるかどうかを判定する。

【0278】

ステップS116において、注目電子チケットに基づく権利が、回数制限付きの権利でないと判定された場合、ステップS117に進み、チケット授受制御部21は、ステップS112でチケット検査装置5_sから受信した乱数 r と、ステップS115で得た注目電子チケットのチケット有効性部（図4（B））に含まれる有効性証明用秘密鍵 VSK_n を、署名処理部24に供給し、乱数 r に対する電子署名 $SG(r)$ を生成させる。

【0279】

即ち、この場合、署名処理部24は、有効性証明用秘密鍵 VSK_n を用いて、乱数 r の一方方向性関数値 $h(r)$ を復号処理することにより、乱数 r に対する電子署名 $SG(r)=D(VSK_n, h(r))$ を生成し、この電子署名 $SG(r)$ を、注目電子チケットの有効性を表す有効性証明用秘密鍵 VSK_n の存在を証明する権利証明用署名として、チケット授受制御部21に供給する。

【0280】

チケット授受制御部21は、署名処理部24から、権利証明用署名 $SG(r)$ を受信すると、ステップS118に進み、その権利証明用署名 $SG(r)$ を、チケット検

査装置 5_s に送信し、ステップ S 1 2 5 に進む。

【0 2 8 1】

一方、ステップ S 1 1 6 において、注目電子チケットに基づく権利が、回数制限付きの権利であると判定された場合、ステップ S 1 1 9 に進み、電子チケットの権利証明を行うのかどうか判定される。なお、この判定は、例えば、ユーザによるチケット保持装置 4_u の操作に基づいて行われる。

【0 2 8 2】

ステップ S 1 1 9 において、権利証明を行うと判定された場合、即ち、例えば、注目電子チケットが、列車の乗車券であり、列車の中で、乗車券を所有していることの確認のために、その乗車券を、車掌に提示しようとしている場合、ステップ S 1 2 0 に進み、チケット授受制御部 2 1 は、ステップ S 1 1 2 でチケット検査装置 5_s から受信した乱数 r と、ステップ S 1 1 5 で得た注目電子チケットのチケット有効性部（図 4（B））に含まれる有効性証明用秘密鍵 VSK_n および付加情報を、署名処理部 2 4 に供給し、乱数 r と付加情報に含まれる使用回数 c に対する電子署名 $SG(r, c)$ を生成させる。

【0 2 8 3】

即ち、この場合、署名処理部 2 4 は、有効性証明用秘密鍵 VSK_n を用いて、乱数 r と付加情報に含まれる使用回数 c の一方向性関数値 $h(r, c)$ を復号処理することにより、乱数 r と使用回数 c に対する電子署名 $SG(r, c) = D(VSK_n, h(r, c))$ を生成し、この電子署名 $SG(r, c)$ を、注目電子チケットの有効性を表す有効性証明用秘密鍵 VSK_n の存在を証明する権利証明用署名として、チケット授受制御部 2 1 に供給する。

【0 2 8 4】

チケット授受制御部 2 1 は、署名処理部 2 4 から、権利証明用署名 $SG(r, c)$ を受信すると、ステップ S 1 2 1 に進み、その権利証明用署名 $SG(r)$ を、チケット有効性部の付加情報に含まれる使用回数 c とともに、チケット検査装置 5_s に送信し、ステップ S 1 2 5 に進む。

【0 2 8 5】

一方、ステップ S 1 1 9 において、電子チケットの権利証明を行うのではない

と判定された場合、即ち、電子チケットの権利行使が行われる場合（例えば、注目電子チケットが、列車の1回限りの乗車券や回数券であり、列車に乗車するために、ユーザが改札を通ろうとしている場合）、ステップS122に進み、チケット授受制御部21は、ステップS112でチケット検査装置5_sから受信した乱数 r と、ステップS115で得た注目電子チケットのチケット有効性部（図4（B））に含まれる有効性証明用秘密鍵 VSK_n および付加情報を、署名処理部24に供給するとともに、権利行使を行うことを表す行使コード e を、署名処理部24に供給する。なお、行使コード e は、例えば、チケット保持装置4_uとチケット検査装置5_sとの間で、あらかじめ定められているものとする。

【0286】

さらに、ステップS122において、チケット授受制御部21は、署名処理部24に、乱数 r 、付加情報に含まれる使用回数 c 、および行使コード e に対する電子署名 $SG(r, c, e)$ を生成させる。

【0287】

即ち、この場合、署名処理部24は、有効性証明用秘密鍵 VSK_n を用いて、乱数 r 、付加情報に含まれる使用回数 c 、および行使コード e の一方方向性関数値 $h(r, c, e)$ を復号処理することにより、乱数 r 、使用回数 c 、および行使コード e に対する電子署名 $SG(r, c, e) = D(VSK_n, h(r, c, e))$ を生成し、この電子署名 $SG(r, c, e)$ を、注目電子チケットの有効性を表す有効性証明用秘密鍵 VSK_n の存在を証明する権利証明用署名として、チケット授受制御部21に供給する。

【0288】

チケット授受制御部21は、署名処理部24から、権利証明用署名 $SG(r, c, e)$ を受信すると、ステップS123に進み、その権利証明用署名 $SG(r, c, e)$ を、チケット有効性部の付加情報に含まれる使用回数 c とともに、チケット検査装置5_sに送信し、ステップS124に進む。

【0289】

ステップS124では、チケット授受制御部21は、注目電子チケットにおけるチケット有効性部の付加情報に含まれる使用回数 c を1だけインクリメントし、ステップS125に進む。

【0290】

ステップS125では、管理部27は、ステップS114で管理情報から抽出した、注目電子チケットのチケット有効性部の暗号化に用いられていた子共通鍵 CK_j を更新する。即ち、管理部27は、乱数発生部23に乱数を発生させ、その乱数から、新たな子共通鍵 CK'_j を生成して、管理情報における元の子共通鍵 CK_j に上書きすることにより、新たな管理情報を得る。

【0291】

そして、ステップS126に進み、管理部27は、チケット授受制御部21から、注目電子チケットのチケット有効性部（このチケット有効性部の付加情報に含まれる使用回数 c は、ステップS122で更新されている場合がある）を取得し、そのチケット有効性部を、新たな子共通鍵 CK'_j とともに、共通鍵暗号処理部29に供給して暗号化させる。即ち、この場合、共通鍵暗号処理部29は、注目電子チケットのチケット有効性部29を、新たな子共通鍵 CK'_j で暗号化し、その結果得られる暗号化チケット有効性部を、管理部27に供給する。

【0292】

ステップS126では、さらに、管理部27が、共通鍵暗号処理部29から供給される暗号化チケット有効性部を、ストレージ部28の注目電子チケットの暗号化チケット有効性部に上書きし、ステップS127に進む。

【0293】

ステップS127では、管理部27は、乱数発生部23に乱数を発生させ、その乱数から、新たな親共通鍵PKを生成して、親共通鍵記憶部27の記憶内容を、その新たな親共通鍵PKで更新する（親共通鍵記憶部27に、新たな親共通鍵PKを上書きする）。

【0294】

そして、ステップS128に進み、管理部27は、新たな親共通鍵PKと、ステップS125で得た新たな管理情報とを、共通鍵暗号処理部29に供給し、その新たな管理情報を、新たな親共通鍵PKで暗号化させる。さらに、ステップS128では、管理部27は、その暗号化された新たな管理情報を、ストレージ部28に上書きする形で記憶させ、チケットの権利行使／証明処理を終了する。

【 0 2 9 5 】

次に、図 1 7 は、図 1 のチケット検査装置 5_sの構成例を示している。

【 0 2 9 6 】

チケット検査装置 5_sは、電子チケットに基づく権利が行使される際や、その権利の行使中に、サービス提供者が、その電子チケットを検査するための機能を有する。具体的には、チケット検査装置 5_sは、チケット保持装置 4_uから、電子チケットの一部であるチケット権利条項部を受け取り、その正当性を確認する機能を有する。さらに、チケット検査装置 5_sは、チケット保持装置 4_uがチケット有効性部を保持していることを、チャレンジアンドレスポンスの認証方法によって確認する機能を有する。

【 0 2 9 7 】

なお、チケット検査装置 5_sは、上述のように、電子チケットを検査する機能を有することから、ユーザが、他のユーザ等から電子チケットを譲受する際に、その譲受前または譲受後の電子チケットが有効であるかどうかの確認に用いることも可能である。従って、以下説明するチケット検査装置 5_sは、それ自体単独で使用する他、チケット保持装置 4_uに内蔵させて使用することも可能である。

【 0 2 9 8 】

チケット検査制御部 3 1 は、チケット保持装置 4_uが保持している電子チケットを検査する、後述するチケット検査処理を行うにあたり、各ブロックと通信しながら、必要な制御を行う。

【 0 2 9 9 】

乱数発生部 3 2 は、チケット検査制御部 3 1 の制御にしたがって、乱数を発生し、チケット検査制御部 3 1 に供給する。

【 0 3 0 0 】

検査内容記憶部 3 3 には、チケット検査装置 5_sを有するサービス提供者がサービスの提供のために必要な条件（以下、適宜、サービス条件という）を記憶させる。ここで、例えば、サービス提供者がイベント開催のサービスを提供し、チケット検査装置 5_sが、イベント会場への入場をチェックするものであるとすれば、開催日時や、場所、イベント名等が、サービス条件に該当する。なお、チケ

ット検査装置 5_sの用途等に応じて、検査内容記憶部 33 は省略可能である。検査内容記憶部 33 が設けられていない場合は、サービス条件が設定されていないものとして扱われる。

【0301】

署名処理部 34 は、チケット検査制御部 31 の制御にしたがい、必要に応じて、署名検証用公開鍵記憶部 35 に記憶された署名検証用公開鍵 P_{CA}等を用いて、電子署名に関する処理を行う。

【0302】

署名検証用公開鍵記憶部 35 は、チケット管理センタ 1 が公開している署名検証用公開鍵 P_{CA}をあらかじめ取得して記憶しており、その記憶している署名検証用公開鍵 P_{CA}を、必要に応じて、署名処理部 34 に供給する。

【0303】

表示部 36 は、チケット検査制御部 31 の制御にしたがって、検査する電子チケットの有効性や内容等を表示する。なお、表示部 36 も、検査内容記憶部 33 と同様に、チケット検査装置 5_sの用途等に応じて、省略可能である。

【0304】

次に、図 18 のフローチャートを参照して、図 17 のチケット検査装置 5_sにおいて、チケット保持装置 4_uが保持している電子チケットを検査する場合に行われるチケット検査処理について説明する。

【0305】

チケット検査処理では、まず最初に、ステップ S131 において、チケット検査制御部 31 は、チケット保持装置 4_uがチケットの権利行使／証明処理（図 16）を行うことにより、ステップ S111 で送信してくる注目電子チケットのチケット権利条項部を受信し、ステップ S132 に進む。

【0306】

ステップ S132 では、チケット検査制御部 31 は、ステップ S131 で受信したチケット権利条項部の正当性を確認する、図 11 で説明したチケット権利条項部の確認処理を行い、ステップ S133 に進む。

【0307】

ステップS133では、チケット検査制御部31は、ステップS131で受信したチケット権利条項部の正当性が確認されたかどうかを判定し、正当性を確認することができなかったと判定した場合、ステップS147に進み、チケット検査制御部31は、チケット権利条項部が改竄等されていることにより、チケット権利条項部の正当性を確認することができなかったとして、サービスを提供することができないこと（サービス提供不可）を認識し、チケット検査処理を終了する。

【0308】

この場合、チケット保持装置4_uのユーザは、サービス提供者からサービスの提供を受けることができない。即ち、例えば、チケット検査装置5_sが列車に乗車するための改札である場合には、チケット保持装置4_uのユーザは、その入場を拒否される。

【0309】

一方、ステップS133において、チケット権利条項部の正当性を確認することができたと判定された場合、ステップS134に進み、チケット検査制御部31は、正当性が確認されたチケット権利条項部（図4（C））におけるチケット権利条項TIが、検査内容記憶部33に記憶されているサービス条件を満足する（サービス条件に合致する）かどうかを判定する。なお、チケット検査装置5_sが、例えば、チケット保持装置4_uに内蔵され、電子チケットを譲受する際に、その電子チケットの有効性の検査に用いられる場合には、ステップS134の処理はスキップされ、ステップS135に進む。

【0310】

ステップS134において、チケット権利条項部におけるチケット権利条項TIがサービス条件を満足しないと判定された場合、即ち、例えば、チケット検査装置5_sが列車に乗車するための改札であるのに対して、ステップS131で受信したチケット権利条項部を有する電子チケットがイベントの入場券である場合、ステップS147に進み、チケット検査制御部31は、サービスを提供することができないことを認識し、チケット検査処理を終了する。

【0311】

この場合も、チケット保持装置 4_u のユーザは、サービス提供者からサービスの提供を受けることができない。

【0312】

一方、ステップ S 134 において、チケット権利条項部におけるチケット権利条項 TI がサービス条件を満足すると判定された場合、ステップ S 135 に進み、チケット検査制御部 31 は、乱数発生部 32 を制御することにより、チャレンジアンドレスポンスの方法による認証を行うための乱数 r を発生させ、ステップ S 136 に進む。ステップ S 136 では、チケット検査制御部 31 は、ステップ S 135 で得た乱数 r を、チケット保持装置 4_u に送信し、ステップ S 137 に進む。

【0313】

ステップ S 137 では、チケット検査制御部 31 は、ステップ S 131 で受信した注目電子チケットのチケット権利条項部におけるチケット権利条項 TI を参照することにより、注目電子チケットに基づく権利が、使用回数の制限されているもの、即ち、回数制限付きの権利であるかどうかを判定する。

【0314】

ステップ S 137 において、注目電子チケットに基づく権利が、回数制限付きの権利でないと判定された場合、ステップ S 138 に進み、チケット検査制御部 31 は、チケット保持装置 4_u が、上述のチケットの権利行使／証明処理（図 16）を行うことによって、ステップ S 118 で送信してくる権利証明用署名 $SG(r)$ を受信する。

【0315】

そして、ステップ S 139 に進み、チケット検査制御部 31 は、ステップ S 138 で受信した権利証明用署名 $SG(r)$ の署名確認を行う。

【0316】

即ち、チケット検査制御部 31 は、正当性の確認されたチケット権利条項部（図 4（C））から、有効性検証用公開鍵 VPK_n を抽出し、権利証明用署名 $SG(r)$ とともに、署名処理部 34 に供給して、権利証明用署名 $SG(r)$ の署名確認を行わせる。

【 0 3 1 7 】

この場合、署名処理部 3 4 は、権利証明用署名 $SG(r)$ を、有効性検証用公開鍵 VPK_n で暗号化処理し、その暗号化結果と、ステップ S 1 3 6 で得た乱数 r との一致性を判定する。そして、署名処理部 3 4 は、その一致性の判定結果を、チケット検査制御部 3 1 に供給する。

【 0 3 1 8 】

ここで、権利証明用署名 $SG(r)$ は、チケット保持装置 4_u が、上述のチケットの権利行使／証明処理（図 1 6）を行うことにより、ステップ S 1 1 7 において、有効性証明用秘密鍵 VSK_n を用いて、乱数 r の一方向性関数値 $h(r)$ を復号処理して得られるものであるから、チケット保持装置 4_u および注目電子チケットが正当なものであれば、権利証明用署名 $SG(r) = D(VSK_n, h(r))$ を、有効性検証用公開鍵 VPK_n で暗号化処理した暗号化結果 $E(VPK_n, SG(r))$ と、乱数 r の一方向性関数値 $h(r)$ とは一致し、署名処理部 3 4 では、一致性があると判定されることになる。

【 0 3 1 9 】

チケット検査制御部 3 1 は、署名処理部 3 4 から一致性の判定結果を受信すると、ステップ S 1 4 5 に進み、その一致性の判定結果に基づき、注目電子チケットに基づく権利が有効なものかどうかを判定する。ステップ S 1 4 5 において、注目電子チケットに基づく権利が有効なものでないと判定された場合、即ち、有効性検証用公開鍵 VPK_n による権利証明用署名 $SG(r)$ の暗号化結果と、ステップ S 1 3 6 で得た乱数 r との一致性が認められず、従って、チケット保持装置 4_u に、注目電子チケットの有効性を表す有効性証明用秘密鍵 VSK_n が存在することが認められない場合、ステップ S 1 4 7 に進み、チケット検査制御部 3 1 は、サービスを提供することができないことを認識し、チケット検査処理を終了する。

【 0 3 2 0 】

この場合、チケット保持装置 4_u のユーザは、サービス提供者からサービスの提供を受けることができない。

【 0 3 2 1 】

一方、ステップ S 1 4 5 において、注目電子チケットに基づく権利が有効なものであると判定された場合、即ち、有効性検証用公開鍵 VPK_n による権利証明用署

名SG(r)の暗号化結果と、ステップS 1 3 6で得た乱数rとの一致性が認められ、従って、チケット保持装置4_uに、注目電子チケットの有効性を表す有効性証明用秘密鍵VSK_nが存在すると認められる場合、ステップS 1 4 6に進み、チケット検査制御部3 1は、サービスを提供することができること（サービス提供可）を認識し、チケット検査処理を終了する。

【0 3 2 2】

この場合、チケット保持装置4_uのユーザは、サービス提供者からサービスの提供を受けることができる。

【0 3 2 3】

一方、ステップS 1 3 7において、注目電子チケットに基づく権利が、回数制限付きの権利であると判定された場合、ステップS 1 4 0に進み、権利証明しようとしている電子チケットの検査を行うのかが判定される。なお、チケット検査装置5_sには、例えば、権利証明または権利行使のうちのいずれについての検査を行うのかが、あらかじめ設定されており、ステップS 1 4 0の判定は、その設定に基づいて行われる。

【0 3 2 4】

ステップS 1 4 0において、権利証明しようとしている電子チケットの検査を行うと判定された場合、ステップS 1 4 1に進み、チケット検査制御部3 1は、チケット保持装置4_uが、上述のチケットの権利行使／証明処理（図1 6）を行うことによって、ステップS 1 2 1で送信してくる権利証明用署名SG(r,c)と使用回数cを受信する。

【0 3 2 5】

そして、ステップS 1 4 2に進み、チケット検査制御部3 1は、ステップS 1 4 1で受信した権利証明用署名SG(r,c)の署名確認を行う。

【0 3 2 6】

即ち、チケット検査制御部3 1は、正当性の確認されたチケット権利条項部（図4（C））から、有効性検証用公開鍵VPK_nを抽出し、権利証明用署名SG(r,c)および使用回数cとともに、署名処理部3 4に供給して、権利証明用署名SG(r,c)の署名確認を行わせる。

【 0 3 2 7 】

この場合、署名処理部 3 4 は、権利証明用署名 $SG(r, c)$ を、有効性検証用公開鍵 VPK_n で暗号化処理し、その暗号化結果と、ステップ S 1 3 6 で得た乱数 r および使用回数 c との一致性を判定する。そして、署名処理部 3 4 は、その一致性の判定結果を、チケット検査制御部 3 1 に供給する。

【 0 3 2 8 】

ここで、権利証明用署名 $SG(r, c)$ は、チケット保持装置 4_u が、上述のチケットの権利行使／証明処理（図 1 6）を行うことにより、ステップ S 1 2 0 において、有効性証明用秘密鍵 VSK_n を用いて、乱数 r および使用回数 c の一方向性関数値 $h(r, c)$ を復号処理して得られるものであるから、チケット保持装置 4_u および注目電子チケットが正当なものであれば、権利証明用署名 $SG(r, c) = D(VSK_n, h(r, c))$ を、有効性検証用公開鍵 VPK_n で暗号化処理した暗号化結果 $E(VPK_n, SG(r, c))$ と、乱数 r および使用回数 c の一方向性関数値 $h(r, c)$ とは一致し、署名処理部 3 4 では、一致性があると判定されることになる。

【 0 3 2 9 】

チケット検査制御部 3 1 は、署名処理部 3 4 から一致性の判定結果を受信すると、ステップ S 1 4 5 に進み、その一致性の判定結果に基づき、注目電子チケットに基づく権利が有効なものかどうかを判定する。ステップ S 1 4 5 において、注目電子チケットに基づく権利が有効なものでないと判定された場合、即ち、有効性検証用公開鍵 VPK_n による権利証明用署名 $SG(r, c)$ の暗号化結果と、乱数 r および使用回数 c との一致性が認められず、従って、チケット保持装置 4_u に、注目電子チケットの有効性を表す有効性証明用秘密鍵 VSK_n が存在することが認められない場合、ステップ S 1 4 7 に進み、チケット検査制御部 3 1 は、表示部 3 6 に、電子チケットが無効である旨を表示させ、チケット検査処理を終了する。

【 0 3 3 0 】

この場合、チケット保持装置 4_u のユーザは、サービス提供者からサービスの提供を受けることができない。

【 0 3 3 1 】

なお、注目電子チケットに基づく権利が、回数制限付き権利である場合、ステ

ステップ S 1 4 5 では、有効性検証用公開鍵 VPK_n による権利証明用署名 $SG(r, c)$ の暗号化結果と、乱数 r および使用回数 c との一致性が認められないときの他、その一致性が認められても、使用回数 c が、注目電子チケットのチケット権利条項部のチケット権利条項 TI に記述されている使用回数の制限値を越えているときには、注目電子チケットに基づく権利が有効なものでないと判定される。

【 0 3 3 2 】

また、ステップ S 1 4 5 では、有効期限がある電子チケットについては、現在の日時が、注目電子チケットのチケット権利条項部のチケット権利条項 TI に記述されている有効期限を越えていないかどうかとも判定され、越えている場合には、注目電子チケットに基づく権利が有効なものでないと判定される。

【 0 3 3 3 】

一方、ステップ S 1 4 5 において、注目電子チケットに基づく権利が有効なものであると判定された場合、即ち、有効性検証用公開鍵 VPK_n による権利証明用署名 $SG(r, c)$ の暗号化結果と、乱数 r および使用回数 c との一致性が認められ、従って、チケット保持装置 4_u に、注目電子チケットの有効性を表す有効性証明用秘密鍵 VSK_n が存在すると認められる場合であって、かつ、使用回数 c が、注目電子チケットのチケット権利条項部のチケット権利条項 TI に記述されている使用回数の制限値を越えていない場合、ステップ S 1 4 6 に進み、チケット検査制御部 3 1 は、サービスを提供することができることを認識し、チケット検査処理を終了する。

【 0 3 3 4 】

この場合、チケット保持装置 4_u のユーザは、サービス提供者からサービスの提供を受けることができる。

【 0 3 3 5 】

一方、ステップ S 1 4 0 において、権利証明しようとしている電子チケットの検査を行うのではないと判定された場合、即ち、権利行使しようとしている電子チケットの検査を行う場合（例えば、ユーザが、乗車券である電子チケットによって改札を通ろうとしている際に、その電子チケットの検査を行う場合）、ステップ S 1 4 3 に進み、チケット検査制御部 3 1 は、チケット保持装置 4_u が、上

述のチケットの権利行使／証明処理（図16）を行うことによって、ステップS123で送信してくる権利証明用署名 $SG(r, c, e)$ と使用回数 c を受信する。

【0336】

そして、ステップS144に進み、チケット検査制御部31は、ステップS143で受信した権利証明用署名 $SG(r, c, e)$ の署名確認を行う。

【0337】

即ち、チケット検査制御部31は、正当性の確認されたチケット権利条項部（図4（C））から、有効性検証用公開鍵 VPK_n を抽出し、権利証明用署名 $SG(r, c, e)$ および使用回数 c とともに、署名処理部34に供給して、権利証明用署名 $SG(r, c, e)$ の署名確認を行わせる。

【0338】

この場合、署名処理部34は、権利証明用署名 $SG(r, c, e)$ を、有効性検証用公開鍵 VPK_n で暗号化处理し、その暗号化結果と、ステップS136で得た乱数 r 、使用回数 c 、行使コード e との一致性を判定する。そして、署名処理部34は、その一致性の判定結果を、チケット検査制御部31に供給する。

【0339】

ここで、権利証明用署名 $SG(r, c, e)$ は、チケット保持装置4_uが、上述のチケットの権利行使／証明処理（図16）を行うことにより、ステップS122において、有効性証明用秘密鍵 VSK_n を用いて、乱数 r 、使用回数 c 、および行使コード e の一方方向性関数値 $h(r, c, e)$ を復号処理して得られるものであるから、チケット保持装置4_uおよび注目電子チケットが正当なものであれば、権利証明用署名 $SG(r, c, e) = D(VSK_n, h(r, c, e))$ を、有効性検証用公開鍵 VPK_n で暗号化处理した暗号化結果 $E(VPK_n, SG(r, c, e))$ と、乱数 r 、使用回数 c 、および行使コード e の一方方向性関数値 $h(r, c, e)$ とは一致し、署名処理部34では、一致性があると判定されることになる。

【0340】

チケット検査制御部31は、署名処理部34から一致性の判定結果を受信すると、ステップS145に進み、その一致性の判定結果に基づき、注目電子チケットに基づく権利が有効なものかどうかを判定する。ステップS145において、

注目電子チケットに基づく権利が有効なものでないと判定された場合、即ち、有効性検証用公開鍵 VPK_n による権利証明用署名 $SG(r,c,r)$ の暗号化結果と、乱数 r 、使用回数 c 、および行使コード e との一致性が認められず、従って、チケット保持装置 4_u に、注目電子チケットの有効性を表す有効性証明用秘密鍵 VSK_n が存在することが認められない場合、あるいは、チケット保持装置 4_u からの権利証明用署名 SG に、正当な行使コード e が存在することが認められない場合、ステップ $S147$ に進み、チケット検査制御部 31 は、サービスを提供することができないことを認識し、チケット検査処理を終了する。

【0341】

この場合、チケット保持装置 4_u のユーザは、サービス提供者からサービスの提供を受けることができない。

【0342】

なお、権利行使しようとしている電子チケットの検査の場合においても、権利証明しようとしている電子チケットの検査における場合と同様に、ステップ $S145$ では、使用回数 c が、注目電子チケットのチケット権利条項部のチケット権利条項 TI に記述されている使用回数の制限値を越えているかどうかや、現在の日時が、注目電子チケットのチケット権利条項部のチケット権利条項 TI に記述されている有効期限を越えていないかどうか等も判定される。

【0343】

一方、ステップ $S145$ において、注目電子チケットに基づく権利が有効なものであると判定された場合、即ち、有効性検証用公開鍵 VPK_n による権利証明用署名 $SG(r,c,e)$ の暗号化結果と、乱数 r 、使用回数 c 、および行使コード e との一致性が認められ、従って、チケット保持装置 4_u に、注目電子チケットの有効性を表す有効性証明用秘密鍵 VSK_n が存在すると認められる場合であって、かつ、使用回数 c が、注目電子チケットのチケット権利条項部のチケット権利条項 TI に記述されている使用回数の制限値を越えておらず、さらに、権利証明用署名 $SG(r,c,e)$ に、正当な行使コード e が含まれている場合、ステップ $S146$ に進み、チケット検査制御部 31 は、サービスを提供することができることを認識し、チケット検査処理を終了する。

【0344】

この場合、チケット保持装置4_uのユーザは、サービス提供者からサービスの提供を受けることができる。

【0345】

次に、上述した一連の処理は、ハードウェアにより行うこともできるし、ソフトウェアにより行うこともできる。一連の処理をソフトウェアによって行う場合には、そのソフトウェアを構成するプログラムが、汎用のコンピュータ等にインストールされる。

【0346】

そこで、図19は、上述した一連の処理を実行するプログラムがインストールされるコンピュータの一実施の形態の構成例を示している。

【0347】

プログラムは、コンピュータに内蔵されている記録媒体としてのハードディスク105やROM103に予め記録しておくことができる。

【0348】

あるいはまた、プログラムは、フロッピーディスク、CD-ROM(Compact Disc Read Only Memory)、MO(Magneto optical)ディスク、DVD(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体111に、一時的あるいは永続的に格納(記録)しておくことができる。このようなリムーバブル記録媒体111は、いわゆるパッケージソフトウェアとして提供することができる。

【0349】

なお、プログラムは、上述したようなリムーバブル記録媒体111からコンピュータにインストールする他、ダウンロードサイトから、デジタル衛星放送用の人工衛星を介して、コンピュータに無線で転送したり、LAN(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを、通信部108で受信し、内蔵するハードディスク105にインストールすることができる。

【0350】

コンピュータは、CPU(Central Processing Unit)102を内蔵している。CPU102には、バス101を介して、入出力インタフェース110が接続されており、CPU102は、入出力インタフェース110を介して、ユーザによって、キーボードや、マウス、マイク等で構成される入力部107が操作等されることにより指令が入力されると、それにしたがって、ROM(Read Only Memory)103に格納されているプログラムを実行する。あるいは、また、CPU102は、ハードディスク105に格納されているプログラム、衛星若しくはネットワークから転送され、通信部108で受信されてハードディスク105にインストールされたプログラム、またはドライブ109に装着されたりムーバブル記録媒体111から読み出されてハードディスク105にインストールされたプログラムを、RAM(Random Access Memory)104にロードして実行する。これにより、CPU102は、上述したフローチャートにしたがった処理、あるいは上述したブロック図の構成により行われる処理を行う。そして、CPU102は、その処理結果を、必要に応じて、例えば、入出力インタフェース110を介して、LCD(Liquid Crystal Display)やスピーカ等で構成される出力部106から出力、あるいは、通信部108から送信、さらには、ハードディスク105に記録等させる。

【0351】

ここで、本明細書において、コンピュータに各種の処理を行わせるためのプログラムを記述する処理ステップは、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく、並列的あるいは個別に実行される処理(例えば、並列処理あるいはオブジェクトによる処理)も含むものである。

【0352】

また、プログラムは、1のコンピュータにより処理されるものであっても良いし、複数のコンピュータによって分散処理されるものであっても良い。さらに、プログラムは、遠方のコンピュータに転送されて実行されるものであっても良い。

【0353】

以上のように、乗車券や、入場券、予約券、会員権許可書、サービス券などの

従来のチケットを電子情報化し、ネットワークなどの電氣的な通信経路を経由してやり取りすることができる電子チケットを、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な有効性証明用秘密鍵 VSK_n を含み、電子チケットの有効性を証明するためのチケット有効性部と、有効性証明用秘密鍵 VSK_n が存在することを検証するのに用いられる有効性検証用公開鍵 VPK_n を含み、有効性証明用秘密鍵 VSK_n によって、その有効性が証明されるチケット権利条項部とによって構成するようにしたので、従来のチケットが有する機能を備える電子チケットの流通を可能にすることができる。

【 0 3 5 4 】

即ち、電子チケットの複製によって、その電子チケットに基づく権利を不正に利用されることを防ぐ機能である「権利複製防止」、匿名の第三者に対する場合も含めて、電子チケットに基づく権利を証明する機能である「権利証明」、電子チケットを使用するユーザの匿名性を保証する機能である「匿名性」、電子チケットに基づく権利を他人に譲ることができる機能である「譲渡性」、および電子チケットに基づく権利の確認を、その電子チケットだけで行うことのできる機能である「完結性」を備える、利便性の高い電子チケットの流通を可能にすることができる。

【 0 3 5 5 】

また、電子チケットのチケット有効性部には、有効性証明用秘密鍵 VSK_n の他、使用回数等の付加情報を含めることができるので、使用回数の制限が可能な、利便性の高い電子チケットを実現することができる。さらに、この場合、使用回数の改竄を防止することができる。

【 0 3 5 6 】

なお、本実施の形態においては、本発明を電子チケットシステムに適用した場合について説明したが、本発明は、その他、例えば、コンピュータに実行させるプログラムにも適用することが可能である。即ち、チケット権利条項部のチケット権利条項 TI に替えてプログラムを配置し、チケット保持装置 4_u を、プログラムの保持装置とするとともに、プログラムの実行に際して、コンピュータにおけるオペレーティングシステム、アプリケーションプログラム、あるいは保持装置

に保持されたプログラムの一部に、チケット検査装置 5_sの機能を持たせて、プログラムの使用等に関する権利の検査を行うようにすることで、プログラムの不正使用を防止する等の、プログラムに関する著作権等の権利を保護することが可能となる。

【 0 3 5 7 】

また、本実施の形態では、公開鍵暗号化方式、共通鍵暗号化方式、および電子署名を利用するようにしたが、これらの公開鍵暗号化方式、共通鍵暗号化方式、および電子署名として採用する具体的なアルゴリズムは、特に限定されるものではない。

【 0 3 5 8 】

【発明の効果】

本発明の情報記録媒体によれば、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データと、秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報とが記録されている。従って、例えば、利便性の高い電子チケットを実現することが可能となる。

【 0 3 5 9 】

本発明の第 1 の情報処理装置および情報処理方法、並びにプログラム記録媒体によれば、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データが生成されるとともに、秘密情報が存在することを検証するのに用いられる検証用パラメータが生成される。そして、検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報が生成され、有効性データと被証明情報とからなる情報セットが外部に出力される。従って、例えば、利便性の高い電子チケットを発行することが可能となる。

【 0 3 6 0 】

本発明の第 2 の情報処理装置および情報処理方法、並びにプログラム記録媒体によれば、それ自体を外部に示すことなく、それが存在することを証明すること

ができるアルゴリズムが適用可能な秘密情報を含む、情報の有効性を証明するための有効性データにおける秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報が、その被証明情報を検査する検査装置に送信される。さらに、秘密情報の存在を証明する証明データが生成され、検査装置に送信される。従って、例えば、電子チケットを、従来の紙等によるチケットと同様に扱うことが可能となる。

【 0 3 6 1 】

本発明の第 3 の情報処理装置および情報処理方法、並びにプログラム記録媒体によれば、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含む、情報の有効性を証明するための有効性データにおける秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報が受信されるとともに、秘密情報の存在を証明する証明データが受信される。そして、証明データと、被証明情報に含まれる検証用パラメータとを用いて、他の装置における秘密情報の存否が判定される。従って、例えば、電子チケットを、従来の紙等によるチケットと同様に扱うことが可能となる。

【 0 3 6 2 】

本発明の情報処理システムによれば、第 1 の情報処理装置において、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含む、情報の有効性を証明するための有効性データが生成されるとともに、秘密情報が存在することを検証するのに用いられる検証用パラメータが生成される。さらに、検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報が生成され、有効性データと被証明情報とからなる情報セットが発行される。第 2 の情報処理装置では、被証明情報が、その被証明情報を検査する第 3 の情報処理装置に送信されるとともに、秘密情報の存在を証明する証明データが生成され、第 3 の情報処理装置に送信される。第 3 の情報処理装置では、第 2 の情報処理装置からの被証明情報が受信されるとともに、第 2 の情報処理装置からの秘密情報の存在を証明する証明データが受信され、証明データと、被証明情報に含まれる検証用パラメータとを用いて、第 2

の情報処理装置における秘密情報の存否が判定される。従って、例えば、利便性の高い電子チケットを流通させることが可能となる。

【図面の簡単な説明】

【図 1】

本発明を適用した電子チケットシステムの一実施の形態の構成例を示す図である。

【図 2】

チケット管理センタ 1 の役割を説明する図である。

【図 3】

チケット管理センタ 1 の役割を説明する図である。

【図 4】

電子チケットのデータフォーマットを示す図である。

【図 5】

チケット発行装置 3_t の構成例を示すブロック図である。

【図 6】

チケット発行処理を説明するフローチャートである。

【図 7】

チケット保持装置 4_u の構成例を示すブロック図である。

【図 8】

ストレージ部 2 8 の記憶内容を示す図である。

【図 9】

チケット譲受処理を説明するフローチャートである。

【図 1 0】

譲受側の認証処理を説明するフローチャートである。

【図 1 1】

チケット権利条項部の確認処理を説明するフローチャートである。

【図 1 2】

チケット追加処理を説明するフローチャートである。

【図 1 3】

チケット譲渡処理を説明するフローチャートである。

【図 14】

譲渡側の認証処理を説明するフローチャートである。

【図 15】

チケット削除処理を説明するフローチャートである。

【図 16】

チケットの権利行使／証明処理を説明するフローチャートである。

【図 17】

チケット検査装置 5_S の構成例を示すブロック図である。

【図 18】

チケット検査処理を説明するフローチャートである。

【図 19】

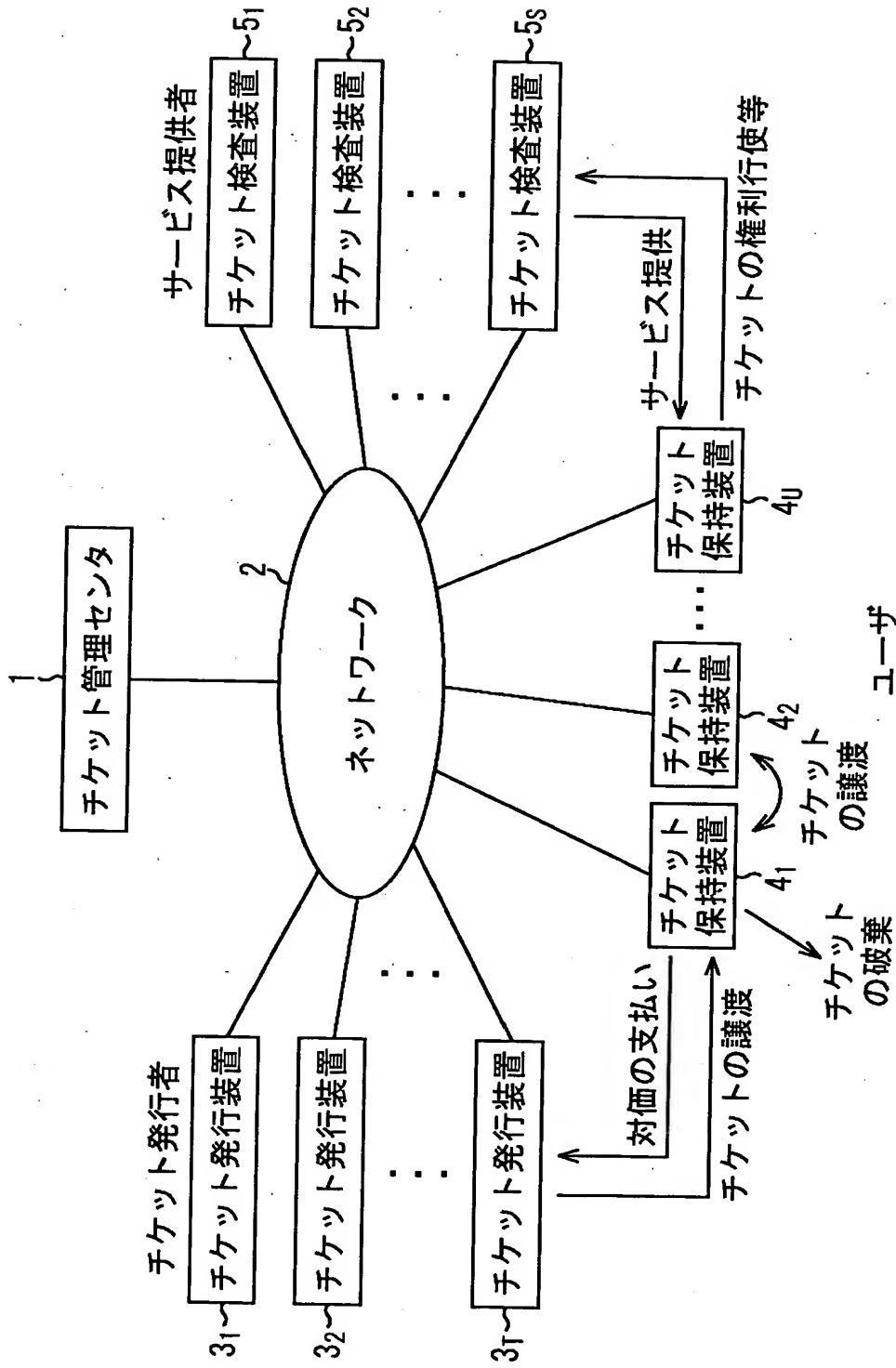
本発明を適用したコンピュータの一実施の形態の構成例を示すブロック図である。

【符号の説明】

1 チケット管理センタ, 2 ネットワーク, 3₁乃至3_T チケット発行装置, 4₁乃至4_U チケット保持装置, 5₁乃至5_S チケット検査装置,
11 チケット条項取得部, 12 発行者証明書取得部, 13 発行者署名生成用秘密鍵取得部, 14 乱数発生部, 15 有効性鍵生成部, 16 条項検証用署名生成部, 17 チケット生成部, 18 チケット保持発行制御部, 21 チケット授受制御部, 22 装置証明書記憶部, 23 乱数発生部, 24 署名処理部, 25 署名検証用公開鍵記憶部, 26 公開鍵暗号処理部, 27 管理部, 27A 親共通鍵記憶部, 28 ストレージ部, 29 共通鍵暗号処理部, 31 チケット検査制御部, 32 乱数発生部, 33 検査内容記憶部, 34 署名処理部, 35 署名検証用公開鍵記憶部, 36 表示部, 101 バス, 102 CPU, 103 ROM, 104 RAM, 105 ハードディスク, 106 出力部, 107 入力部, 108 通信部, 109 ドライブ, 110 入出力インタフェース, 111 リムーバブル記録媒体

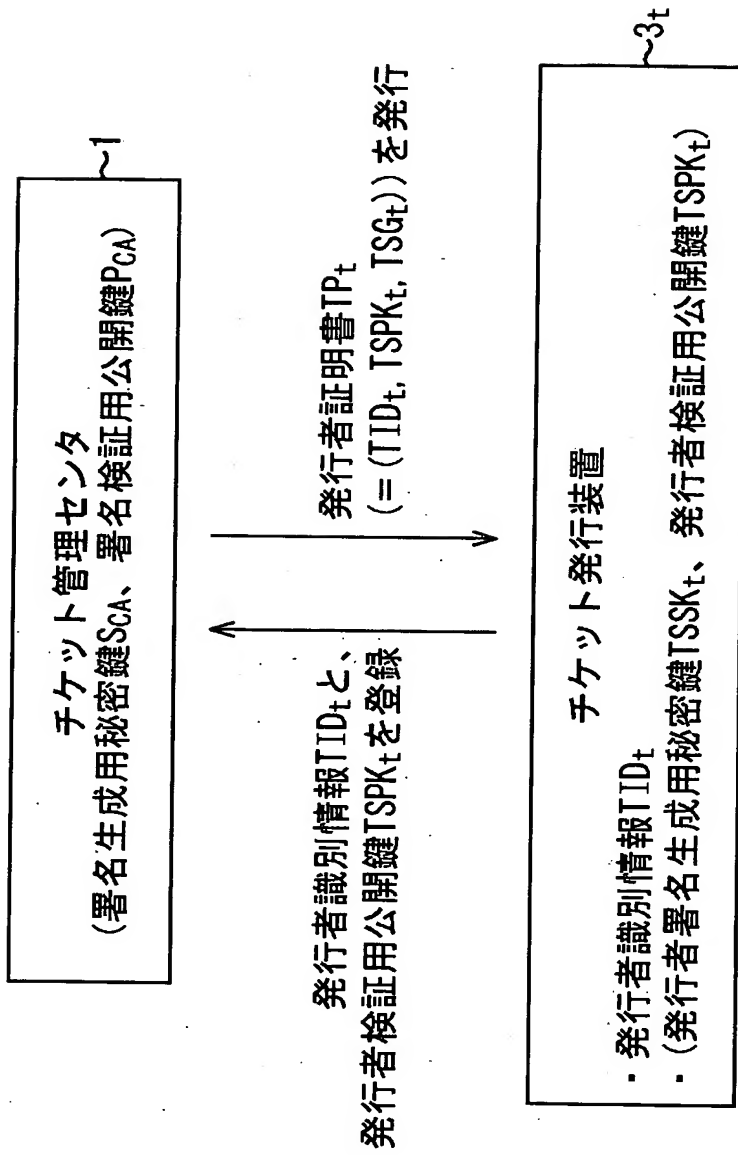
【書類名】 図面

【図 1】

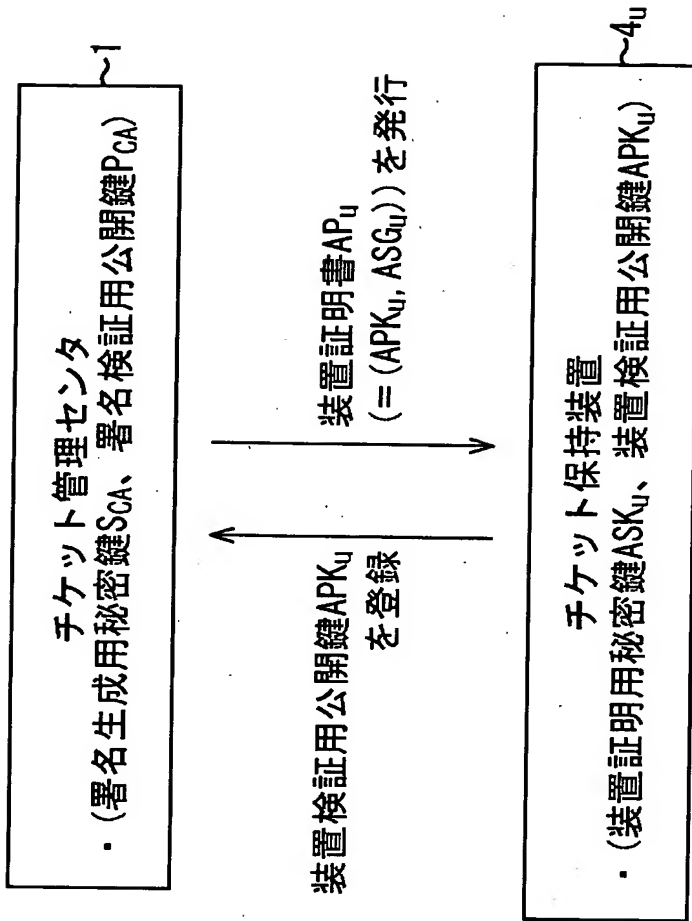


電子チケットシステム

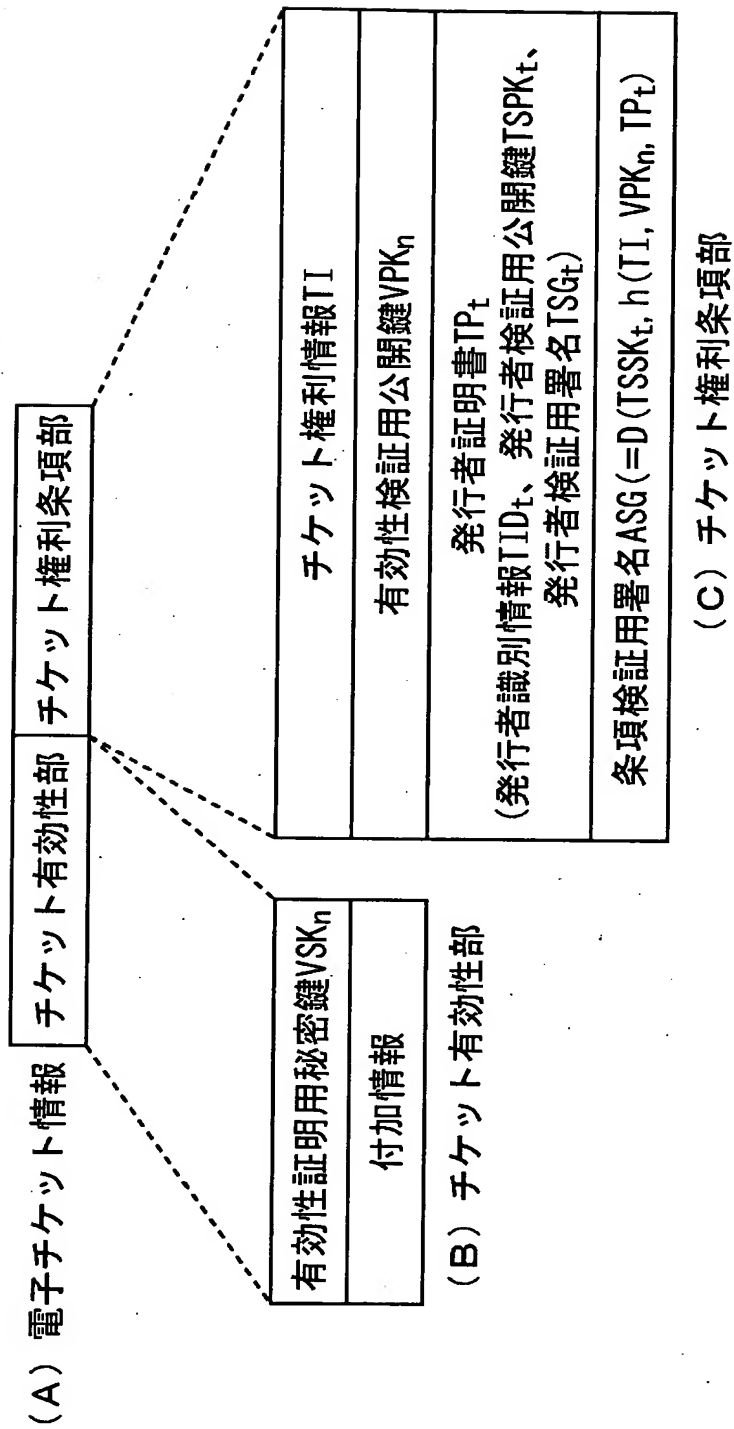
【図 2】



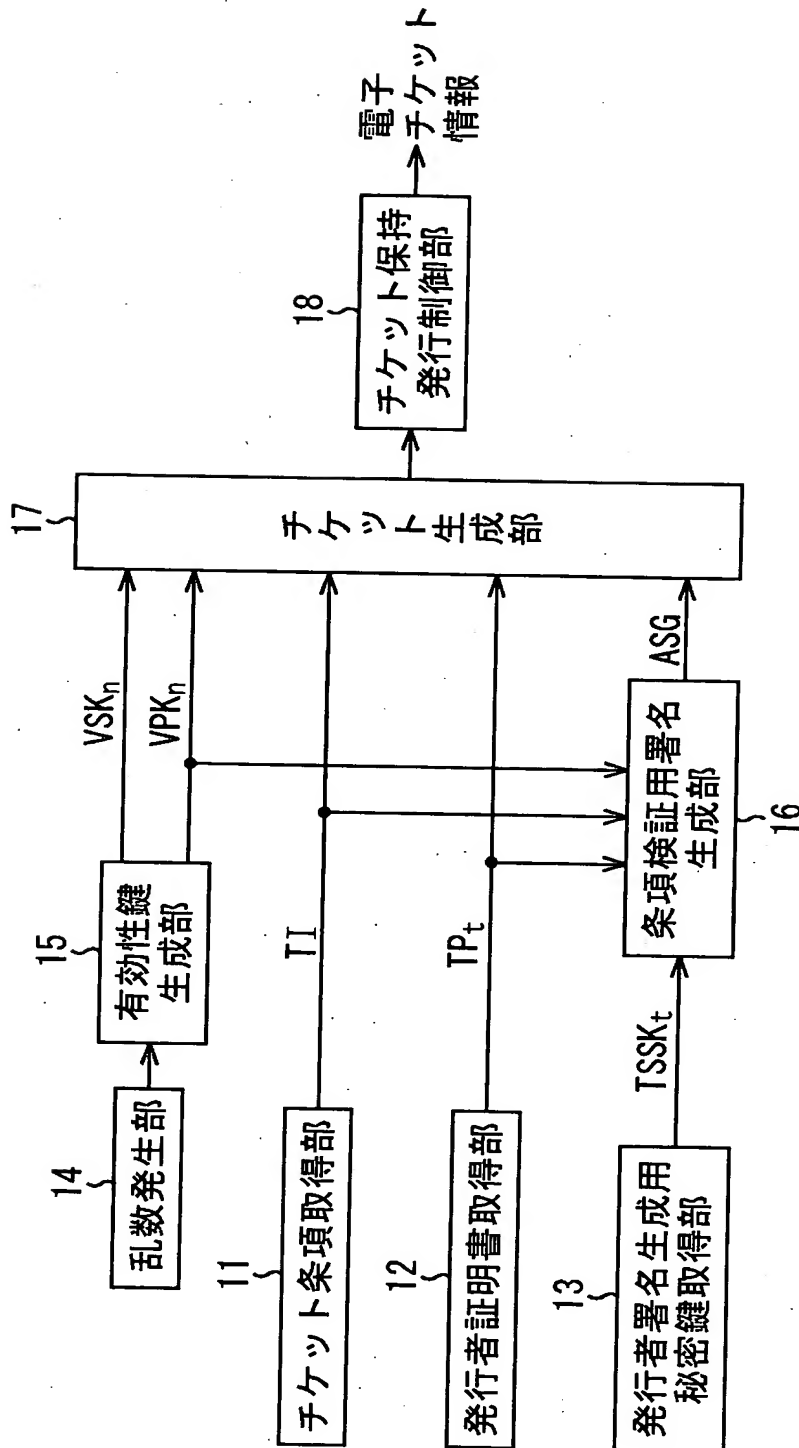
【図 3】



【図 4】

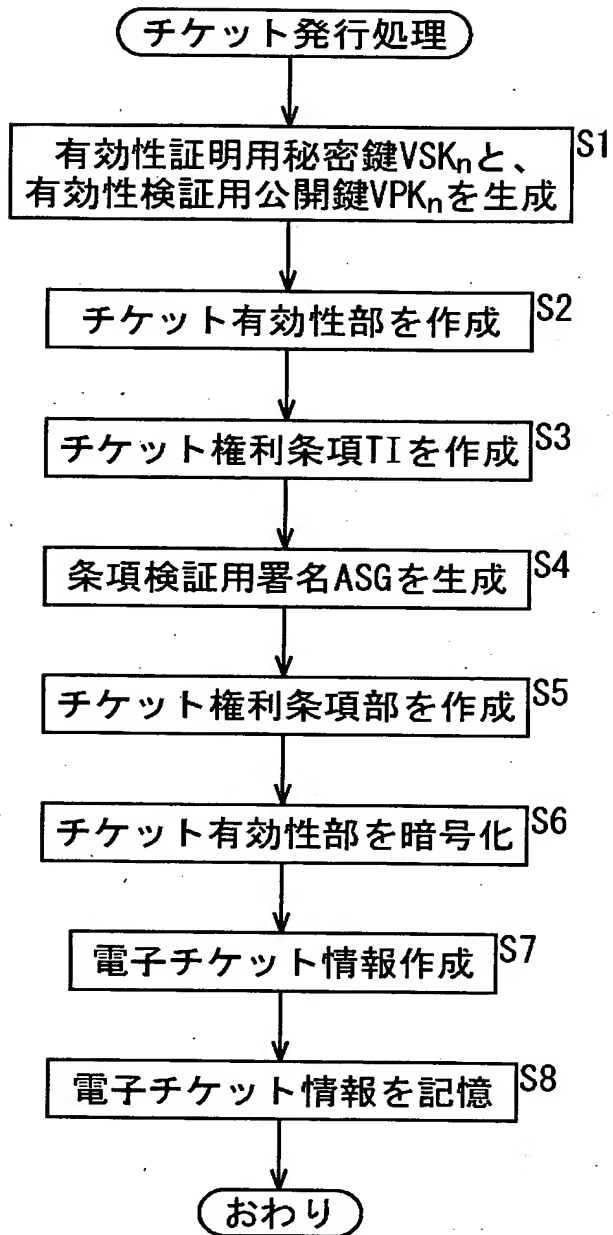


【図 5】

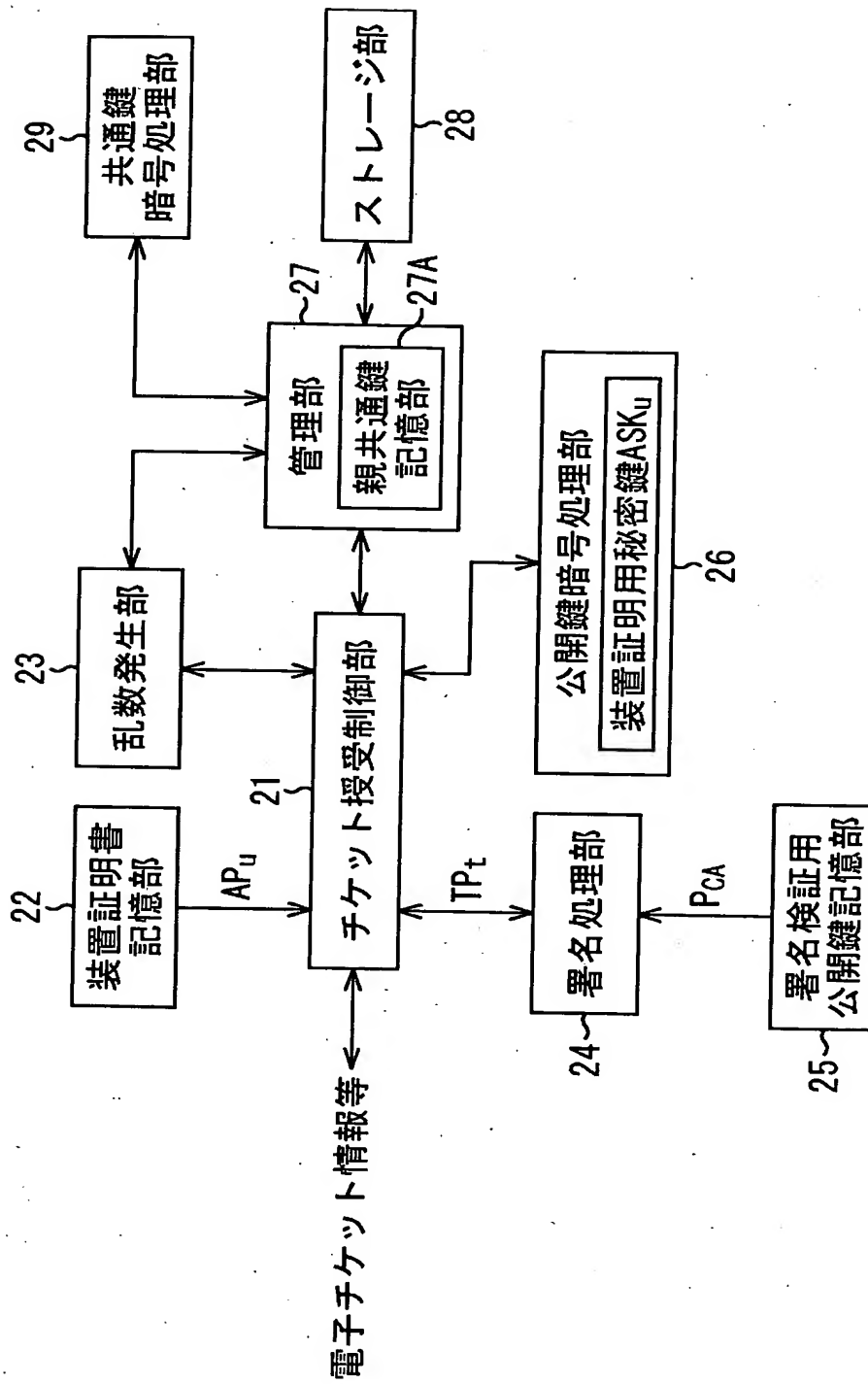


チケット発行装置 3t

【図 6】

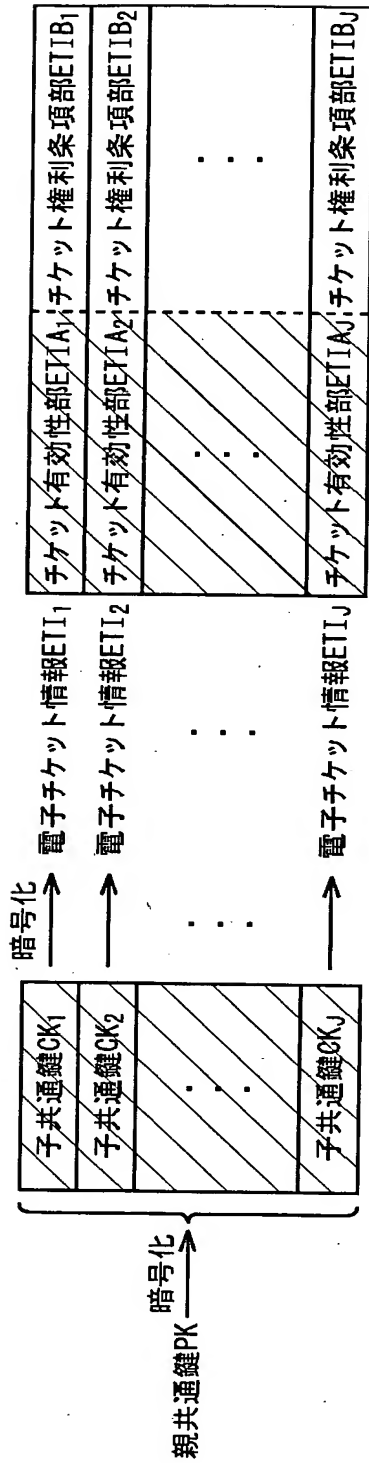


【図 7】



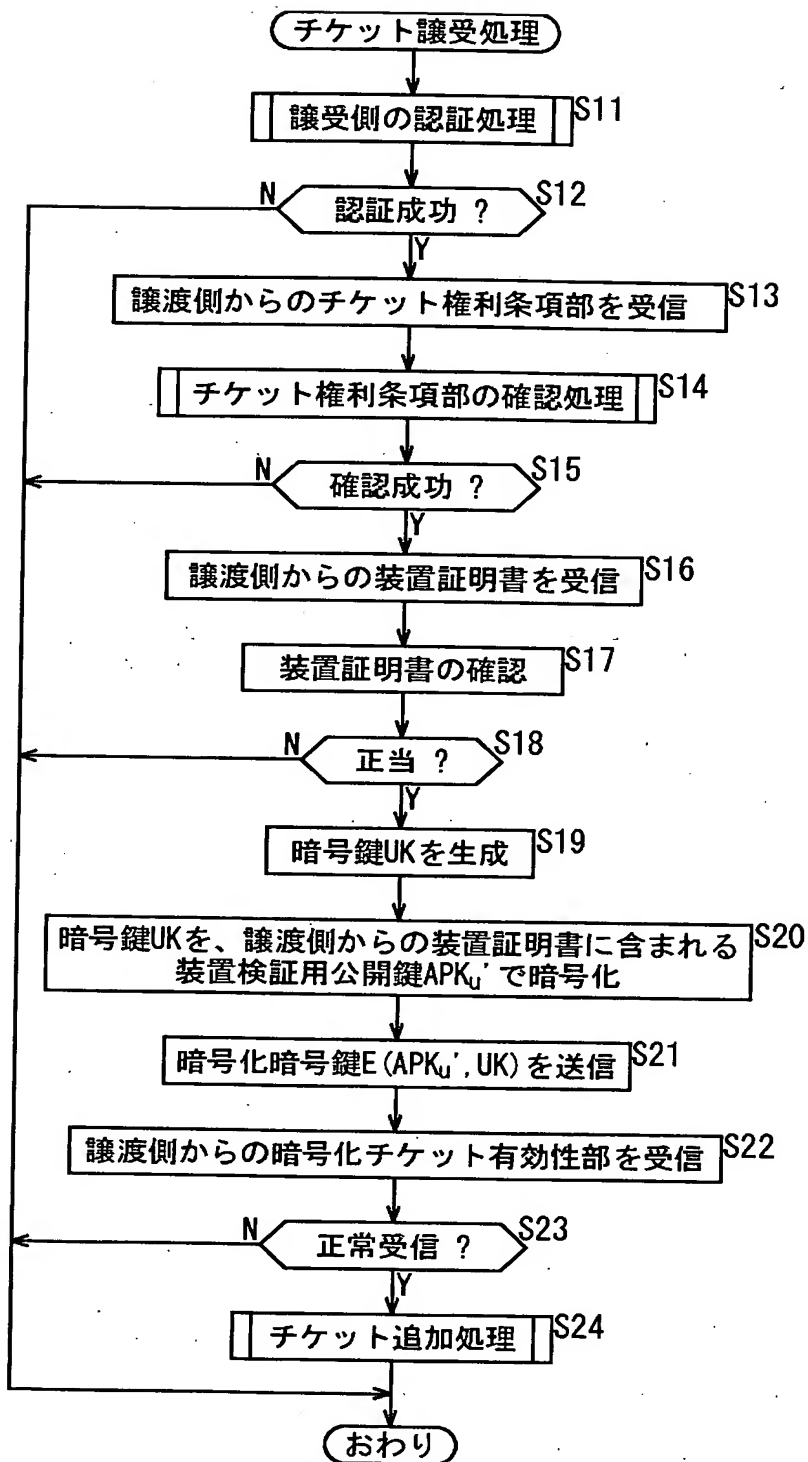
チケット保持装置 4u

【図 8】

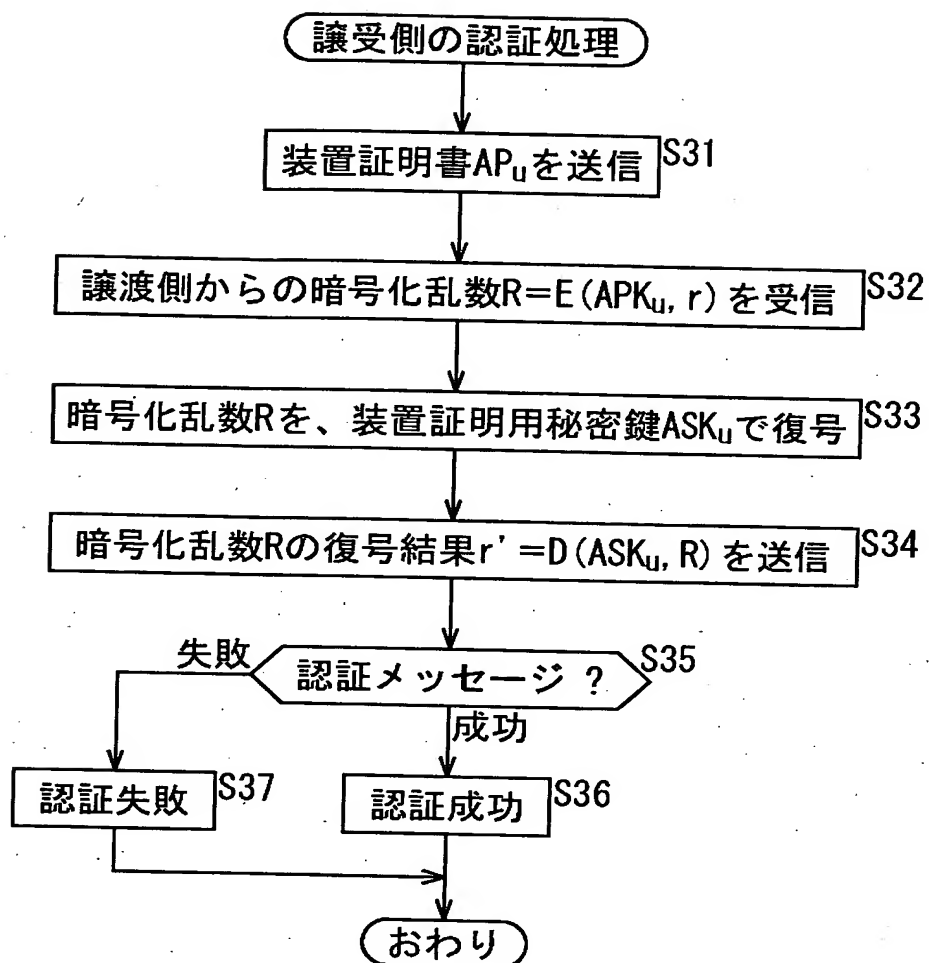


ストレージ部の記憶内容

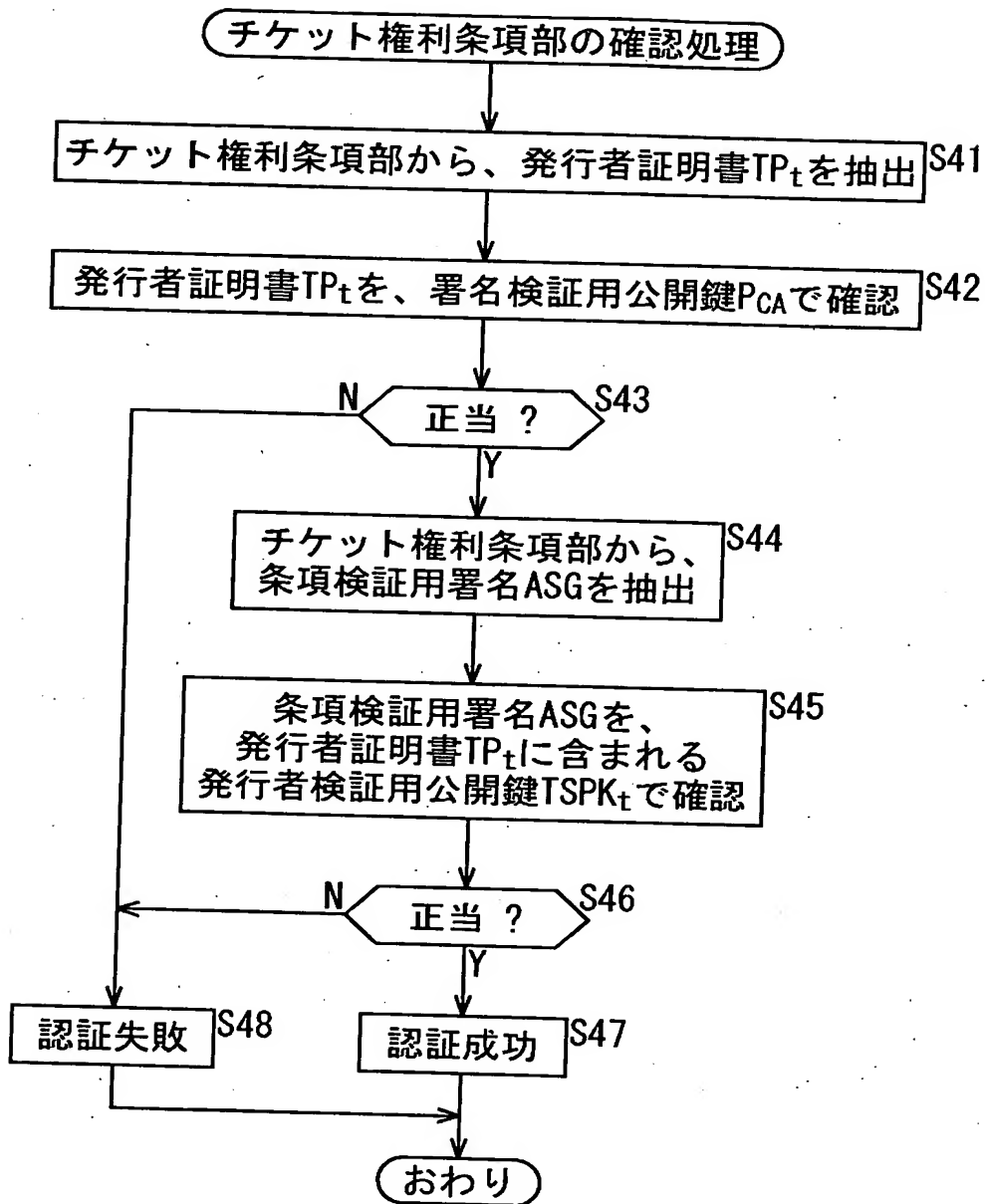
【図 9】



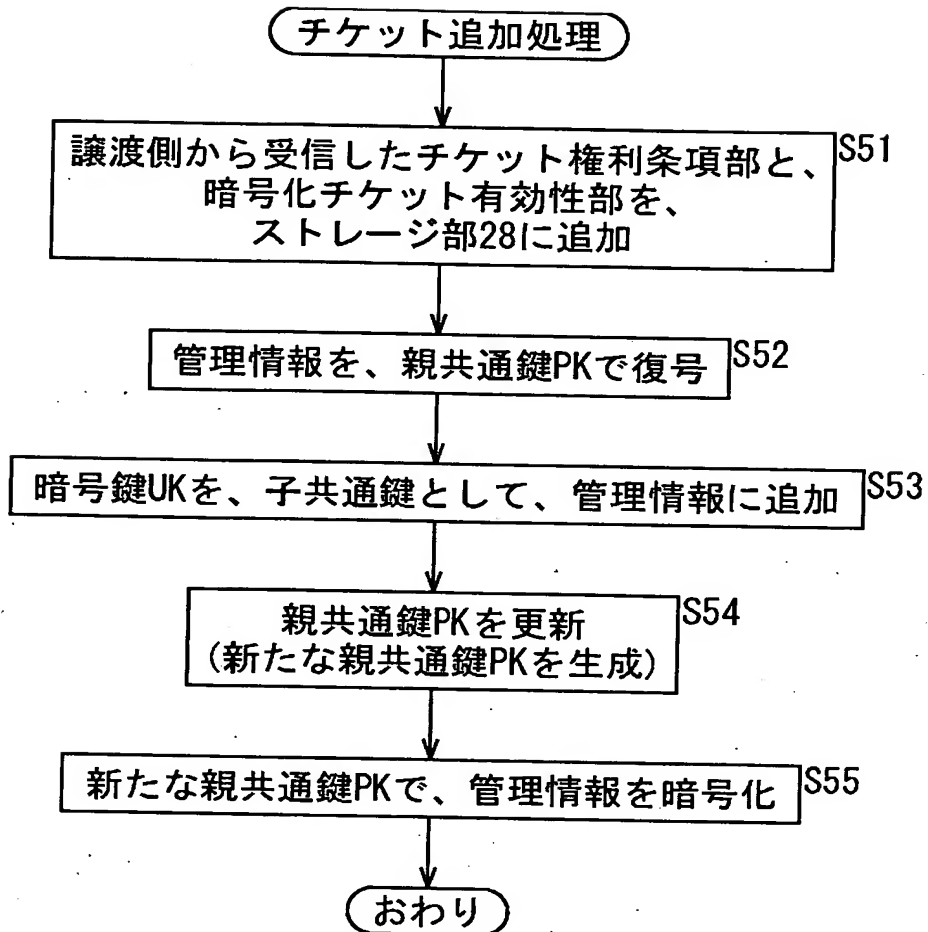
【図 1 0】



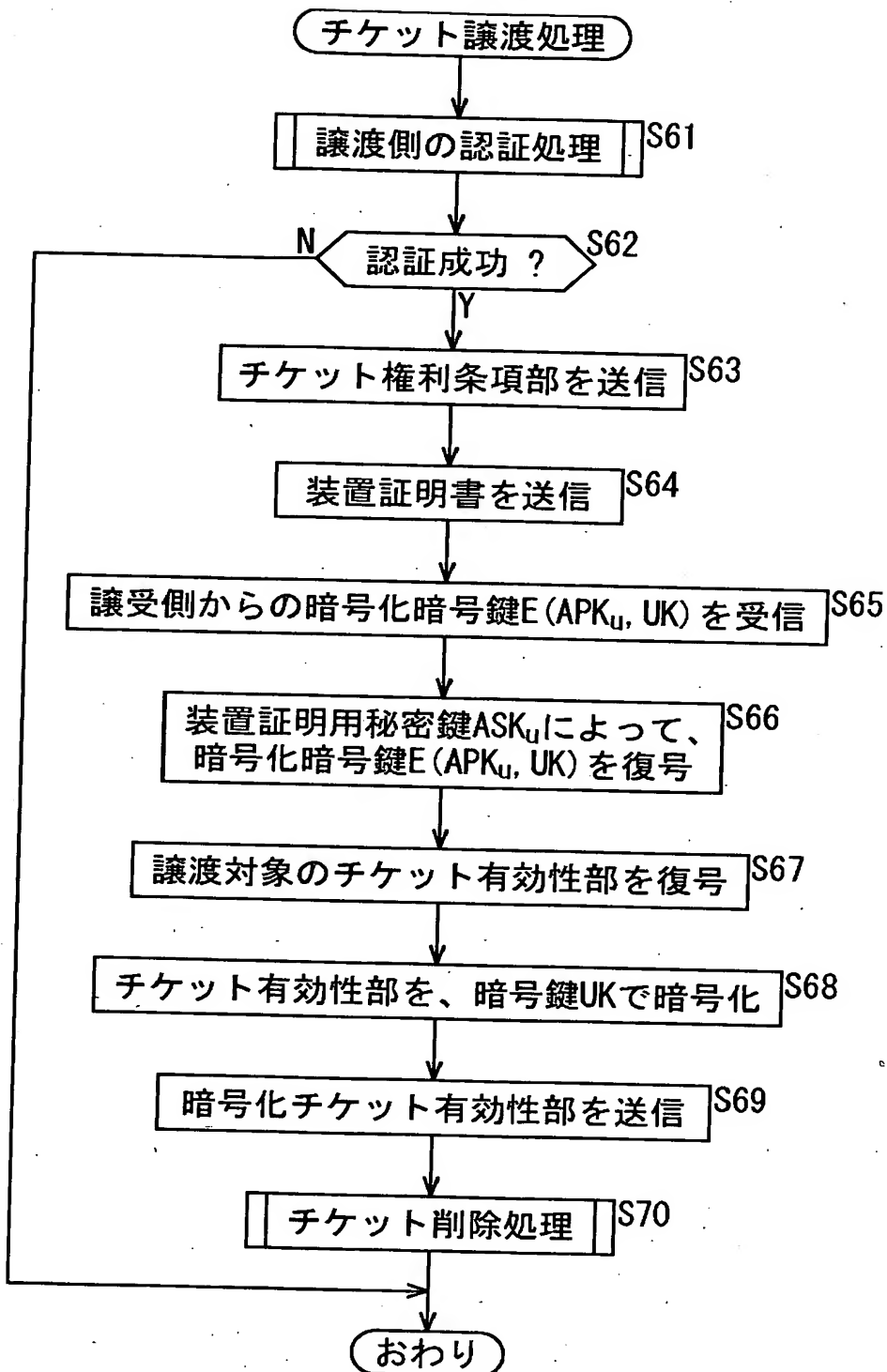
【図 1 1】



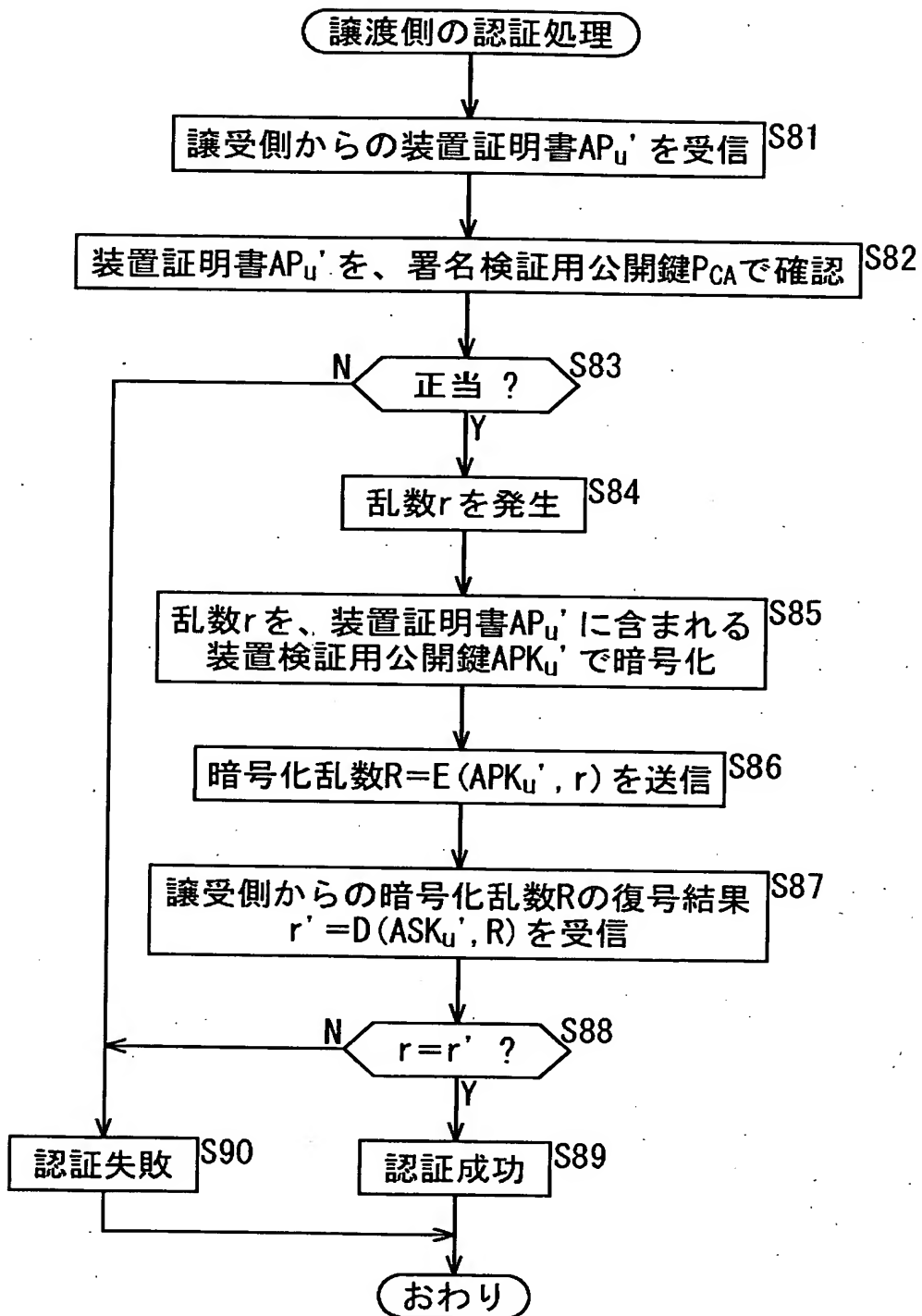
【図 1 2】



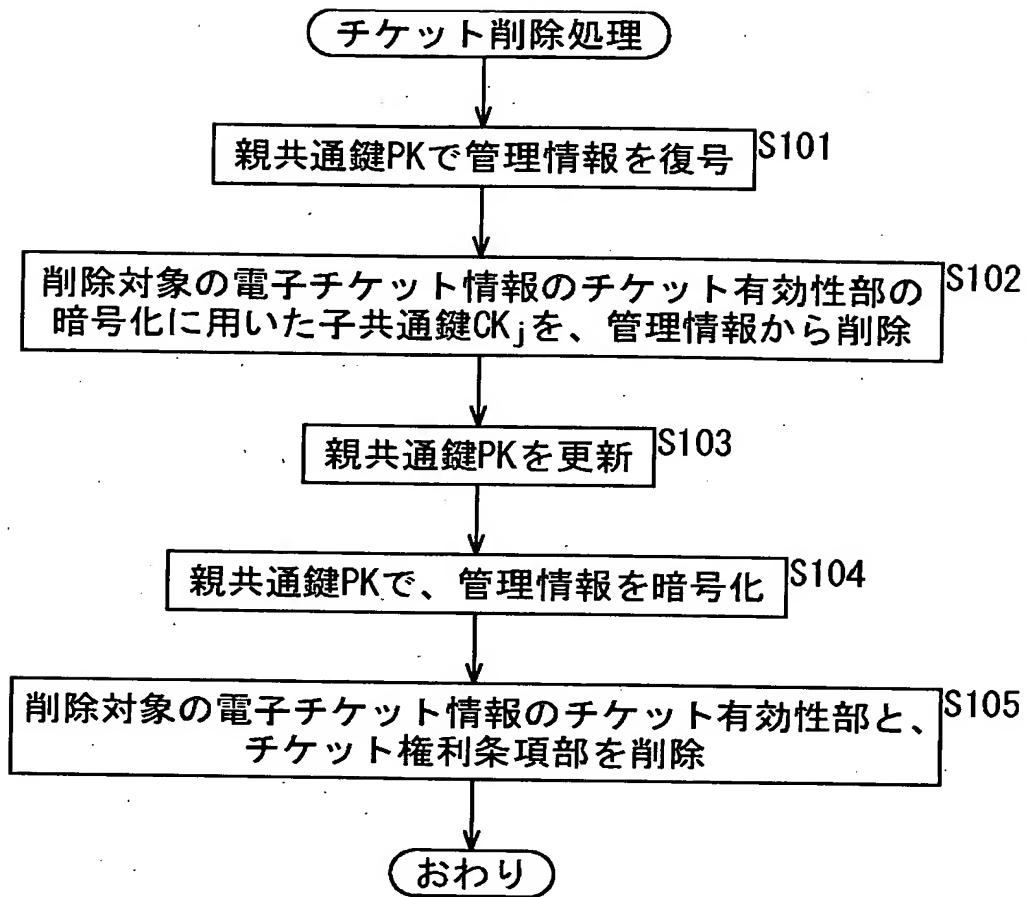
【図 13】



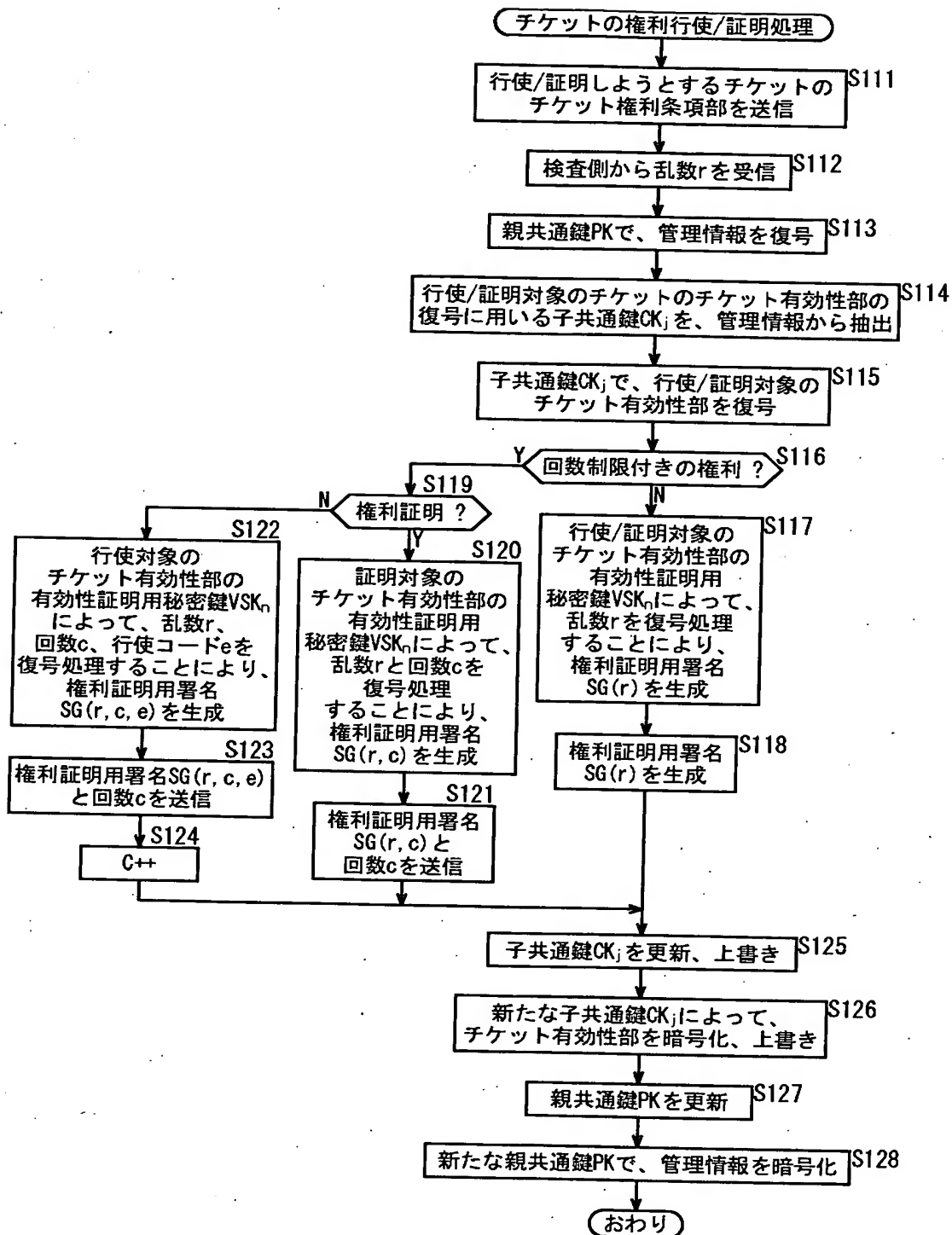
【図 1 4】



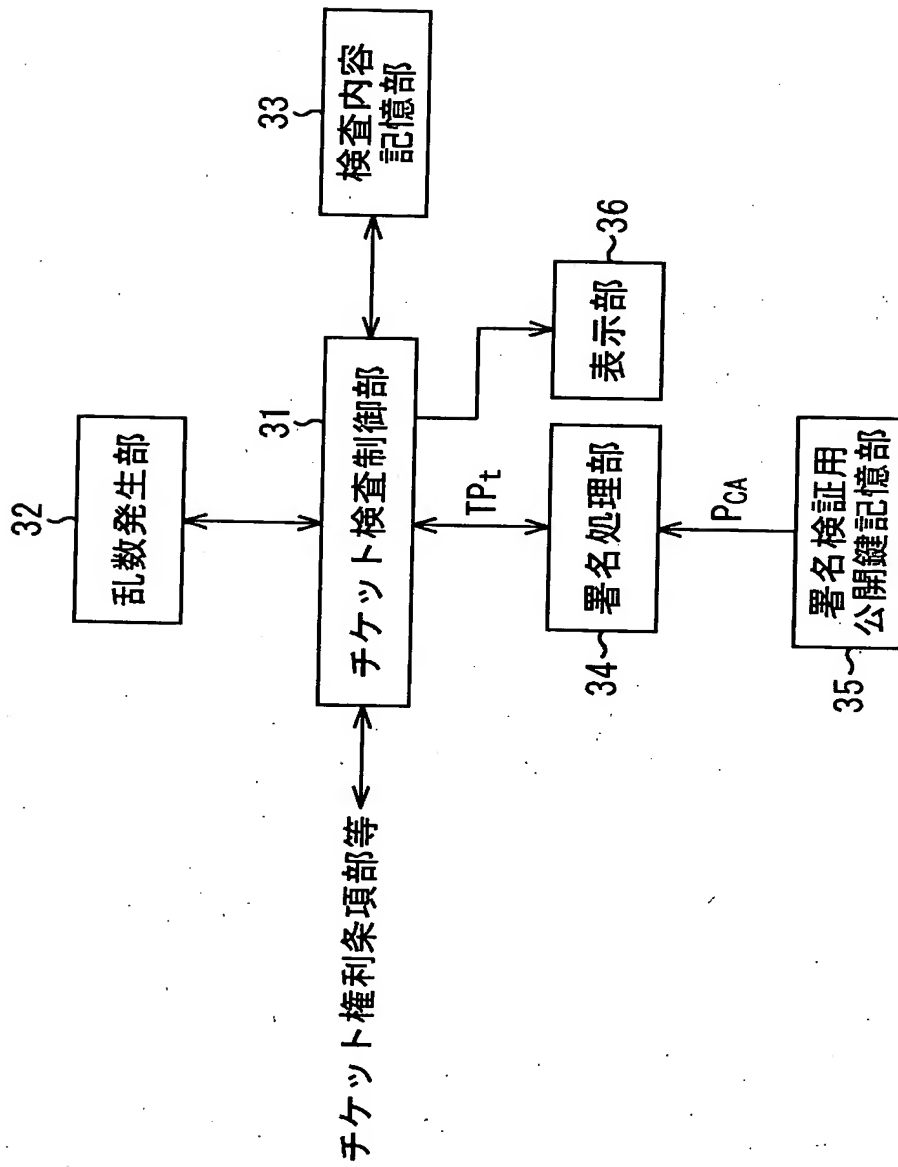
【図 1 5】



【図 16】

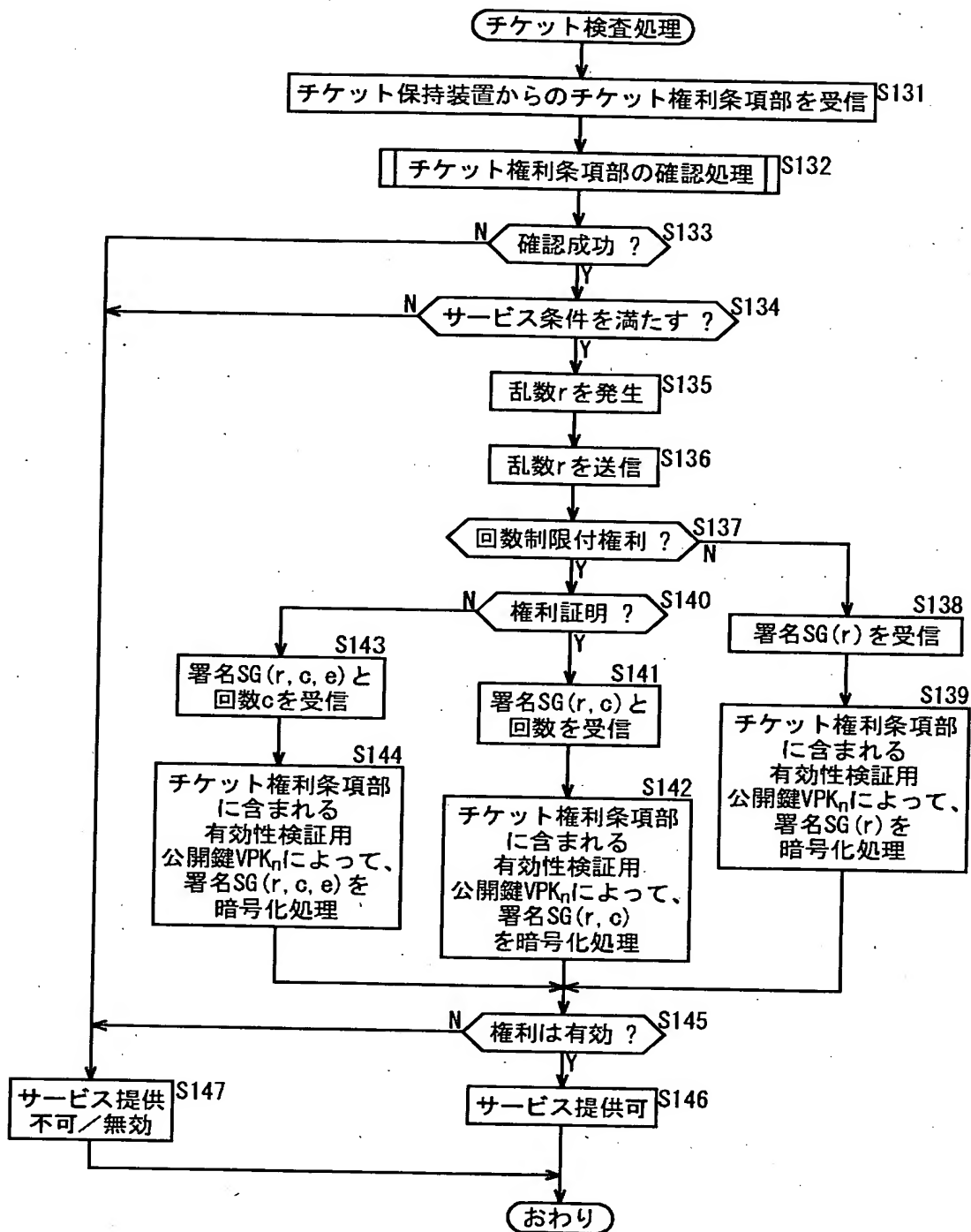


【図 17】

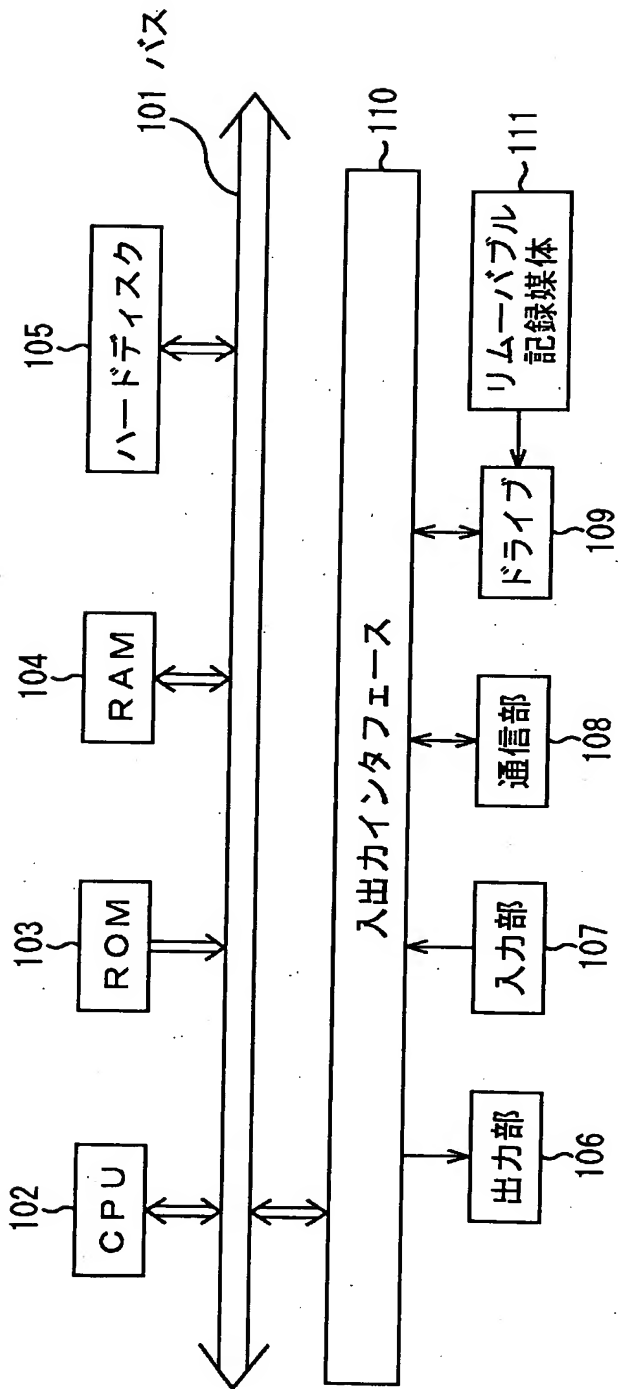


チケット検査装置 5s

【図 18】



【図19】



コンピュータ

【書類名】 要約書

【要約】

【課題】 利便性の高い電子チケットを実現する。

【解決手段】 チケット発行装置 3_tは、それ自体を外部に示すことなく、その存在を証明することができるアルゴリズムが適用可能な秘密鍵を含む有効性データと、その秘密鍵の存在を検証するのに用いられる、その秘密鍵に対応する公開鍵を含み、有効性データによって、その有効性が証明される被証明情報とを生成し、有効性データと被証明情報とからなる電子チケットを発行する。チケット保持装置 4_uは、有効性データにおける秘密鍵の存在を証明する電子署名を生成し、被証明情報とともに、チケット検査装置 5_sに送信する。チケット検査装置 5_sは、チケット保持装置 4_uからの電子署名と、被証明情報に含まれる公開鍵とを用いて、チケット保持装置 4_uにおける秘密鍵の存否を判定する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号

[000002185]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住 所 東京都品川区北品川6丁目7番35号
氏 名 ソニー株式会社